

New Studies of Randomized Augmentation and Additive Preprocessing *

Victor Y. Pan^{[1,2],[a]} and Liang Zhao^{[2],[b]}

^[1] Department of Mathematics and Computer Science
Lehman College of the City University of New York
Bronx, NY 10468 USA

^[2] Ph.D. Programs in Mathematics and Computer Science
The Graduate Center of the City University of New York
New York, NY 10036 USA

^[a] victor.pan@lehman.cuny.edu
<http://comet.lehman.cuny.edu/vpan/>
^[b] lzhao1@gc.cuny.edu

Abstract

- A standard Gaussian random matrix has full rank with probability 1 and is well-conditioned with a probability quite close to 1 and converging to 1 fast as the matrix deviates from square shape and becomes more rectangular.
- If we append sufficiently many standard Gaussian random rows or columns to any matrix A , such that $\|A\| = 1$, then the augmented matrix has full rank with probability 1 and is well-conditioned with a probability close to 1, even if the matrix A is rank deficient or ill-conditioned.
- We specify and prove these properties of augmentation and extend them to additive preprocessing, that is, to adding a product of two rectangular Gaussian matrices.
- By applying our randomization techniques to a matrix that has numerical rank ρ , we accelerate the known algorithms for the approximation of its leading and trailing singular spaces associated with its ρ largest and with all its remaining singular values, respectively.
- Our algorithms use much fewer random parameters and run much faster when various random sparse and structured preprocessors replace Gaussian. Empirically the outputs of the resulting algorithms is as accurate as the outputs under Gaussian preprocessing.
- Our novel *duality techniques* provides formal support, so far missing, for these empirical observations and opens door to *derandomization* of our preprocessing and to further acceleration and simplification of our algorithms by using more efficient sparse and structured preprocessors.
- Our techniques and our progress can be applied to various other fundamental matrix computations such as the celebrated low-rank approximation of a matrix by means of random sampling.

2000 Math. Subject Classification: 65F05, 65F35, 15A06, 15A52, 15A12

*Some results of this paper have been presented at the ACM-SIGSAM International Symposium on Symbolic and Algebraic Computation (ISSAC '2011), San Jose, CA, 2011, the 3rd International Conference on Matrix Methods in Mathematics and Applications (MMMA 2011) in Moscow, Russia, June 22-25, 2011, the 7th International Congress on Industrial and Applied Mathematics (ICIAM 2011), in Vancouver, British Columbia, Canada, July 18-22, 2011, the SIAM International Conference on Linear Algebra, in Valencia, Spain, June 18-22, 2012, and the Conference on Structured Linear and Multilinear Algebra Problems (SLA2012), in Leuven, Belgium, September 10-14, 2012.

Key Words: Randomized matrix algorithms; Gaussian random matrices; Singular spaces of a matrix; Duality; Derandomization; Sparse and structured preprocessors

1 Introduction

1.1 Randomized augmentation: outline

A standard Gaussian $m \times n$ random matrix, G (hereafter referred to just as *Gaussian*), has full rank with probability 1 (see Theorem B.1). Furthermore the expected spectral norms $\|G\|$ and $\|G^+\|$, G^+ denoting the Moore-Penrose generalized inverse, satisfy the following estimates (see Theorems B.2 and B.3):

- $\mathbb{E}(\|G\|) \approx 2\sqrt{h}$, for $h = \max\{m, n\}$, and
- $\mathbb{E}(\|G^+\|) \leq \frac{e\sqrt{l}}{|m-n|}$ provided that $l = \min\{m, n\}$, $m \neq n$, and $e = 2.71828 \dots$

Thus, for moderate or reasonably large integers m and n , the matrix G can be considered well-conditioned with the confidence growing fast as the integer $|m - n|$ increases from 0. By virtue of part 2 of Theorem B.3, the matrix G can be viewed as well-conditioned even for $m = n$, although with a grain of salt, depending on context.

Motivated by this information, we append sufficiently but reasonably many Gaussian rows or columns to any matrix A , possibly rank deficient or ill-conditioned, but normalized, such that $\|A\| = 1$. (Our approach requires attention to various pitfalls, and in particular it fails without normalization of an input matrix.) Then we prove that the cited properties of a Gaussian matrix also hold for the augmented matrix K and similarly for the matrix $C = A + UV^T$ where U and V are Gaussian matrices.

We, however, prove and confirm empirically that *randomized augmentation* $A \rightarrow K$ above is likely to produce matrices with smaller condition numbers than *randomized additive preprocessing* $A \rightarrow C = A + UV^T$ and than augmentation by appending to a matrix A two blocks of rows and columns simultaneously. These results should help direct properly our randomization.

Its main application area is the computations with rank deficient and ill-conditioned matrices. In particular, suppose we are given a matrix A that has a numerical rank ρ and seek approximate bases for we approximate closely the leading and trailing singular spaces associated with the ρ largest and with all the remaining singular values of that matrix, respectively.

The known numerical algorithms solve these problems by applying pivoting, orthogonalization, or the Singular Value Decomposition (SVD). Orthogonalization and particularly SVD are more costly (and more reliable), but even pivoting takes its toll – it interrupts the stream of arithmetic operations with foreign operations of comparison, involves book-keeping, compromises data locality, increases communication overhead and data dependence, readily destroys matrix structure and sparseness, and threatens or undermines application of block matrix algorithms.

In the next two sections we solve these problems by applying randomized augmentation or additive preprocessing at a much lower randomized computational cost versus the expensive known techniques.

1.2 Randomized sparse and structured preprocessing

Our study has some similarity with the celebrated work on *low-rank approximation* of a matrix by means of random sampling (cf. [HMT11]) and with randomized preprocessing of Gaussian elimination without pivoting¹ in [PQY15]. In particular, similarly to randomized low-rank approximation in [HMT11, Section 11], our techniques, algorithms and their analysis can be extended to the case where preprocessing with Gaussian matrices is replaced by preprocessing with *Semisample Random Fourier Transform*² structured matrices, defined in our Appendix C and [HMT11, Section 11].

¹Hereafter we use the acronym *GENP*.

²Hereafter we use the acronym *SRFT*.

The transition from Gaussian to SRFT preprocessing greatly simplifies the computations, but increases the estimated probability of failure. This estimate, however, seems to be overly pessimistic for most inputs because empirical frequency of failure (observed consistently in our tests and in the tests covered in [HMT11]) was about the same in the cases of Gaussian and SRFT preprocessing.

More generally, our tests (as well as the tests for randomized low-rank approximation by many authors and the tests for GENP in [PQY15]) have consistently produced similar outputs with about the same accuracy when preprocessing with various random sparse and structured matrices (including SRFT matrices as a special subclass) replaced Gaussian preprocessing (cf. Table 7.4).

Formal support for such empirical observations has been a challenge for quite a while, and our simple but novel insight enables us to provide it finally: we prove that *the known estimates for the impact of preprocessing with a Gaussian multiplier onto any input matrix can be extended to preprocessing with any well-conditioned multiplier of full rank onto average input matrix* and consequently onto a statistically typical, that is, almost any input matrix with a narrow class of exceptions. In this basic *Duality Theorem* we assume that average matrix is defined under the Gaussian probability distribution. Such a provision is customary, and it is quite natural in view of the Central Limit Theorem.

Regarding the class of allowed multipliers, the restriction in the theorem is the *mildest possible* and allows us to select sparse and structured multipliers which can be generated and multiplied by an input matrix as fast as one could wish. Thus, besides providing formal support, so far missing, for the cited empirical observations, our results open door to *derandomization* of our preprocessing and to further *acceleration and simplification* of the known algorithms by using more efficient sparse and structured preprocessors.

Our reports [PZa] and [PZb] have furnished such a simple but novel duality techniques also for low-rank approximation and GENP with further extension to Fast Multipole and Conjugate Gradient celebrated algorithms.

1.3 Some related works and further research directions

Our present study continues and enhances the progress in the works [BP94, Section 2.13], [PY07], [PMRT07], [W07], [PIMR08a], [PIMR08b], [PGMQ08], [PY09], [PIMR10], [PQ10], [PQ12], [PQY15], [PQZC], [PQZ13], and [PY09] on increasing the efficiency of matrix algorithms by means of randomized preprocessing. Unlike these earlier works, we support the favorable results of our extensive tests with detailed formal analysis.

Our Algorithms 3.1t and 3.1t+ show that the power of randomized multiplication, studied extensively in [BP94, Section 2.13], [PGMQ08, Section 12.2], [PY09], [HMT11], [PQZ13], [PQY15], [PZ15], [PZa], [PZb], and the references therein, can be enhanced when we combine it with randomized augmentation or additive preprocessing.

The search for such synergistic combinations is a natural and important research challenge. As we have pointed out already, our work should motivate bolder application of sparse and structured preprocessing towards simplification and acceleration of matrix computations. Our progress should motivate efforts for the extension of our techniques and results to other fundamental matrix computations, by following the first steps in these directions in [PZa] and [PZb].

1.4 Organization of the paper

We organize our paper as follows.

In the next subsection and in the Appendix we cover some definitions and auxiliary results. In Sections 2 and 3 we approximate leading and trailing singular spaces of a matrix that has smaller numerical rank by applying our randomization techniques. These two sections make up Part I of our paper, devoted to our algorithms.

In Sections 4 and 5 we estimate the impact of Gaussian augmentation and additive preprocessing on the condition number of a matrix, these estimates imply correctness of our algorithms of Sections 2 and 3. In Section 6 we extend our study to the case of sparse and structured randomization and

present our results on dual randomization. Sections 4–6 form Part II of our paper, devoted to the analysis of our algorithms.

Section 7 covers our numerical tests, which are the contribution of the second author. In Section 8 we summarize our study and discuss some directions for further research. Sections 7 and 8 make up Part III of our paper, devoted to tests, summary, and extension of our algorithms.

1.5 Some basic definitions

Except for Appendix C, we work in the field \mathbb{R} of real numbers, but a large part of our study can be extended to the computations in the field \mathbb{C} of complex numbers (cf. [E88], [ES05], [CD05]).

Hereafter the concepts “large”, “small”, “near”, “close”, “approximate”, “ill-conditioned” and “well-conditioned” are quantified in the context. By saying “likely” we mean with a probability close to 1.

$(B_1 \mid \dots \mid B_k) = (B_j)_{j=1}^k$ denotes a $1 \times k$ block matrix with the blocks B_1, \dots, B_k .

I and I_k denote the $k \times k$ identity matrix.

O and $O_{k,l}$ denote the $k \times l$ matrix filled with zeros.

$\|M\| = \|M\|_2$ is the spectral norm of a matrix M .

For a matrix M having full column rank, $Q(M)$ denotes a unique orthogonal matrix defined by the QR factorization $M = QR$ where $R = R(M)$ is a unique upper triangular square matrix with positive diagonal entries (cf. [GL13, Theorem 5.2.3]).

$\mathcal{G}^{m \times n}$ is the class of Gaussian $m \times n$ matrices.

See some additional definitions in Section 2.1 and the Appendix.

PART I: Randomized Matrix Algorithms

2 Approximation of the Leading Singular Spaces

2.1 Left inverses, matrix bases, nmbs, and singular spaces

An $m \times n$ matrix M has an $n \times m$ left inverse matrix $X = M^{(I)}$ such that $XM = I_n$ if and only if it has full column rank n . (We can compute at first QR factorization $M = QR$ for orthogonal $m \times n$ matrix Q and then a left inverse $M^{(I)} = R^{-1}Q^T$, by performing $O(mn^2)$ flops overall.)

A matrix having full column rank is a *matrix basis* for its range. A matrix basis B for the null space $\mathcal{N}(M)$ is a *null matrix basis* or a *nmb* for the matrix M , denoted $\text{nmb}(M)$. In other words $B = \text{nmb}(M)$ if the matrix B has full column rank and if $\mathcal{R}(B) = \mathcal{N}(M)$.

Suppose that we are given three integers k, m and n , $1 < k < \min\{m, n\}$, an $m \times n$ matrix M of rank ρ , and its SVD

$$M = S_M \Sigma_M T_M^T, \quad (2.1)$$

where S_M and T_M are square orthogonal matrices, $\Sigma_M = \text{diag}(\hat{\Sigma}_M, O_{m-\rho, n-\rho})$ is the diagonal matrix of the singular values,

$$\hat{\Sigma}_M = \text{diag}(\sigma_j(M))_{j=1}^\rho, \quad \sigma_1 = \|M\|, \quad \text{and } \sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_\rho > 0.$$

Partition the matrices S_M , Σ_M , and T_M into their leading and trailing parts as follows,

$$S_M = (S_{k,M} \mid S_{M,k}), \quad \Sigma_M = \text{diag}(\Sigma_{k,M}, \Sigma_{M,k}), \quad \text{and } T_M = (T_{k,M} \mid T_{M,k}), \quad (2.2)$$

where $S_{k,M} \in \mathbb{R}^{m \times k}$, $T_{k,M} \in \mathbb{R}^{n \times k}$, $S_{M,k} \in \mathbb{R}^{m \times (m-k)}$, $T_{M,k} \in \mathbb{R}^{n \times (n-k)}$, $\Sigma_{k,M} = \text{diag}(\sigma_j(M))_{j=1}^k$, and $\Sigma_{M,k} = \text{diag}(\text{diag}(\sigma_j(M))_{j=k+1}^\rho, O_{m-\rho, n-\rho})$.

Now write $\mathbb{S}_{k,M} = \mathcal{R}(S_{k,M})$, $\mathbb{T}_{k,M} = \mathcal{R}(T_{k,M})$, $\mathbb{S}_{M,k} = \mathcal{R}(S_{M,k})$, and $\mathbb{T}_{M,k} = \mathcal{R}(T_{M,k})$.

If $\sigma_k > \sigma_{k+1}$, then $\mathbb{S}_{k,M}$ and $\mathbb{T}_{k,M}$ are the leading left and right singular spaces associated with the k largest singular values of the matrix M , respectively, and $\mathbb{S}_{M,k}$, and $\mathbb{T}_{M,k}$ are the trailing left and right singular spaces associated with the remaining singular values, respectively.

For $k = \rho$, we arrive at *compact SVD*, $M = S_{\rho,M} \Sigma_{\rho,M} T_{\rho,M}^T$ where $\Sigma_{\rho,M} = \hat{\Sigma}_M$.

For a positive tolerance η , a matrix M has η -rank ρ , $\rho = \text{rank}_\eta(M)$, if $\sigma_\rho(M) < \eta \leq \sigma_{\rho+1}(M)$ or, equivalently, if the matrix M can be approximated within the norm bound η by a matrix of rank ρ , but not by a matrix of rank $\rho - 1$. Note that

$$\text{rank}_\eta(M) \leq \text{rank}_{\eta'}(M) \leq \text{rank}(M) \text{ if } \eta \geq \eta'.$$

η -rank is said to be *numerical rank* if η is small (in context).

2.2 Linking approximation of a matrix and of its leading singular space

For an $m \times n$ matrix A having numerical rank ρ , seek approximation to its leading singular space $\mathbb{T}_{\rho,A}$. The following theorem links closely this task to the celebrated task of low-rank approximation of a matrix A , extensively covered in [HMT11].

Theorem 2.1. *Let $\text{rank}(A) = \rho$. Write $\Delta = Q - T_{\rho,A}V$ for a $\rho \times \rho_+$ orthogonal matrix V where $\rho_+ \geq \rho$. Then*

$$\frac{\|AQQ^T - A\|}{\|A\|} \leq (2 + \|\Delta\|)\|\Delta\| + \frac{\sigma_{\rho+1}(A)}{\sigma_1(A)}.$$

Proof. Deduce from the equation $T_A^T T_{\rho,A} = (I_\rho \mid O_{n-\rho,\rho})^T$ that

$$AT_{\rho,A}T_{\rho,A}^T = S_A \Sigma_A T_A^T T_{\rho,A} T_{\rho,A}^T = S_{\rho,A} \Sigma_{\rho,A} T_{\rho,A}^T = A_\rho.$$

Recall that $Q = T_{\rho,A}V + \Delta$, $T_A^T T_{\rho,A} = (I_\rho \mid O_{n-\rho,\rho})^T$, and $A = A_\rho + \bar{A}_\rho$ where $\bar{A}_\rho = S_{\rho,A} \Sigma_{\rho,A} T_{\rho,A}^T$ and $\|\bar{A}_\rho\| \leq \sigma_{\rho+1}(A)$. Combine the above equations and obtain

$$AQQ^T - A = -\bar{A}_\rho + AT_{\rho,A}V\Delta^T + A\Delta(V^T T_{\rho,A}^T + \Delta^T).$$

Now substitute $\|\bar{A}_\rho\| = \sigma_{\rho+1}(A)$ and $\|T_{\rho,A}\| = \|V\| = 1$ and obtain

$$\|AQQ^T - A\| \leq \sigma_{\rho+1}(A) + (2 + \|\Delta\|)\|\Delta\| \|A\|.$$

The theorem follows because $\|A\| = \sigma_1(A)$. □

Remark 2.1. *If the error norm $\|\Delta\|$ of the approximation to the leading singular space $\mathbb{T}_{\rho,A}$ is small, then, by virtue of Theorem 2.1, the relative error of rank- ρ approximation of the matrix A by AQQ^T is also small. Conversely, if the ratio $\frac{\|AQQ^T - A\|}{\|A\|}$ is small, then by applying [HMT11, Algorithm 5.1] one can approximate the matrices $S_{\rho,A} \approx QS_{Q^T A}$ and $T_{\rho,A} \approx QS_{AQ}$ of the leading singular vectors essentially at the cost of computing compact SVDs of the matrices $Q^T A$ and AQ of smaller sizes. Having the matrix $S_{\rho,A}$ approximated, we can readily approximate at first the matrix $\Sigma_{\rho,A} T_{\rho,A}^T = S_{\rho,A}^T A$ and then the matrices $\Sigma_{\rho,A}$ and $T_{\rho,A}$ (thus approximating the leading part of SVD of the matrix A), and similarly if we are given an approximation of the matrix $T_{\rho,A}$. Based on these observations, [HMT11, Section 10.2] readily extends [HMT11, Algorithm 4.1] to randomized computation of the numerical rank of a matrix.*

2.3 Randomized approximation of a leading singular space

Definition 2.1. $\mathbb{E}(v)$ denotes the expected value of a random variable v . $\nu_{m,n}$, $\nu_{F,m,n}$, $\nu_{m,n}^+$, and $\kappa_{m,n}$ denote the random variables $\|G\|$, $\|G\|_F$ (Frobenius norm of G), $\|G^+\|$, and $\kappa(G) = \|G\| \|G^+\|$, respectively, and $\nu_n^+ = \nu_n^+(A)$ denote the norm $\|(A + G)^+\|$ provided that $A \in \mathbb{R}^{n \times n}$ and $G \in \mathcal{G}^{n \times n}$.

Note that $\nu_{n,m} = \nu_{m,n}$, $\nu_{n,m}^+ = \nu_{m,n}^+$, and $\kappa_{n,m} = \kappa_{m,n}$, and assume that the random variables $\nu_{m,n}$, $\nu_{m,n}^+$, $\nu_{F,m,n}$, and ν_n^+ turn into 1 if $m = 0$ or $n = 0$.

By virtue of [SST06, Theorem 3.3], for $n \geq 2$, a real $x > 0$, and a matrix $A \in \mathbb{R}^{n \times n}$, it holds that

$$\text{Probability } \{\nu_n^+ \geq x\} \leq 2.35\sqrt{n}/x. \quad (2.3)$$

Our next task is the approximation of a leading singular space $\mathbb{T}_{\rho,A}$ of a matrix A that has numerical rank ρ . We adopt the technique of *random sampling*, that is, approximate $\mathbb{T}_{\rho,A}$ by the range of the matrix $A^T H$ for a Gaussian $m \times \rho_+$ matrix H and for a nonnegative but not large integer $\rho_+ - \rho$. This technique has been studied in [HMT11] for low-rank approximation of such a matrix A , but our error analysis is a little different because we approximate the space $\mathbb{T}_{\rho,A}$ rather than the matrix A . The following theorem estimates the approximation error.

Theorem 2.2. (Cf. Definition 2.1.) Suppose that an $m \times n$ matrix A has numerical rank ρ , H is an $n \times \rho_+$ Gaussian matrix, $H \in \mathcal{G}^{n \times \rho_+}$, and $m \geq n \geq \rho_+ \geq \rho > 0$. Then with probability 1 there exists an $n \times \rho_+$ matrix X of rank ρ such that $\mathcal{R}(X) = \mathbb{T}_{\rho,A}$ and $\|A^T H - X\| \leq \sigma_{\rho+1}(A) \nu_{n,\rho_+}$.

Proof. Recall equations (2.1) and (2.2), for $M = A$ and $k = \rho = \text{nrnk}(A)$, and write

$$A^T H = A_\rho^T H + \bar{A}_\rho^T H, \quad \bar{A}_\rho = S_{A,\rho} \Sigma_{A,\rho} T_{A,\rho}^T, \quad \text{and} \quad A_\rho = S_{\rho,A} \Sigma_{\rho,A} T_{\rho,A}^T.$$

Then

$$A_\rho^T H = T_{\rho,A} \Sigma_{\rho,A} B \quad \text{and} \quad \|\bar{A}_\rho^T H\| \leq \|\bar{A}_\rho^T\| \|H\| = \sigma_{\rho+1}(A) \nu_{n,\rho_+} \quad (2.4)$$

where $B = S_{\rho,A}^T H$ is a $\rho \times \rho_+$ Gaussian matrix by virtue of Lemma B.1.

Now the theorem follows for $X = A_\rho^T H$ because the matrix $\Sigma_{\rho,A}$ is nonsingular by assumption, and with probability 1 the matrix B has full rank, by virtue of Theorem B.1. \square

The bound $\sigma_{\rho+1}(A) \nu_{n,\rho_+}$ of (2.4) can be large only with a probability close to 0, and one can monitor the approximation error by estimating the ratio $\frac{\|A Q Q^T - A\|}{\|A\|}$ (see Remark 2.1). Probabilistic estimates for this ratio in [HMT11, Sections 10.2 and 10.3] have order $\sigma_{\rho+1}(A)$ and hold with a probability $1 - 3/p^p$ for an oversampling integer $p = \rho_+ - \rho$ if $p \geq 20$.

Theorem 2.2 implies correctness of the following simple randomized algorithm, which is a subalgorithm of [HMT11, Algorithm 4.1].

Algorithm 2.1. (Cf. Remarks 2.2 and 2.3.)

INPUT: Three integers m , n , and ρ_+ such that $m \geq n \geq \rho_+ > 0$, and an $m \times n$ matrix A having numerical rank $\rho \leq \rho_+$.

OUTPUT: An orthogonal $n \times \rho_+$ matrix X , whose range is likely to approximate the leading singular space $\mathbb{T}_{\rho,A}$.

COMPUTATIONS: 1. Generate a Gaussian $n \times \rho_+$ matrix H .
2. Compute and output the $n \times \rho_+$ matrix $X = A^T H$.

The algorithm generates $n\rho_+$ i.i.d. Gaussian values and then performs $(2n - 1)m\rho_+$ flops, but we need only $n + \rho_+$ random parameters and $O(mn \log(\rho_+) + n\rho_+^2)$ flops if we replace the $n \times \rho_+$ Gaussian multiplier H with an $n \times \rho_+$ SRFT structured multiplier. Hereafter we refer to Algorithm 2.1 with a SRFT multiplier as **Algorithm 3.1+**. Then again we can monitor its output error norm by estimating the ratio $\frac{\|A Q Q^T - A\|}{\|A\|}$. According to the study of SRFT multipliers in [HMT11, Section 11], the ratio is large with a probability in $O(1/r)$ if ρ_+ has order $(\rho + \log(n)) \log(\rho)$, but empirically even the choice of $\rho_+ = \rho + 20$ “is adequate in almost all applications”.

Remark 2.2. (Cf. [HMT11, Theorem 9.2].) The approximation of a basis for the leading (as well as trailing) singular spaces is facilitated as the gaps increase between the singular values of the input matrix A . This motivates preprocessing of an input matrix A by means of the power transforms $A \implies B_h = (A A^T)^h A$ for positive integers h because $\sigma_j(B_h) = (\sigma_j(A))^{2h+1}$ for all j .

Remark 2.3. By applying the algorithms of this subsection to the transpose A^T we can approximate the left singular spaces of our input matrix A . If, however, an approximation $Q_T = T_{\rho,A} V + \Delta_T$ to a matrix basis for the right singular space $\mathbb{T}_{\rho,A}$ is already available, then we can readily compute an approximation $A Q_T$ to the matrix basis for the left singular space $\mathbb{S}_{\rho,A}$. Indeed $A Q_T =$

$S_A \Sigma_A T_A^T (T_{\rho,A} V + \Delta_T) = S_A \Sigma_A T_A^T T_{\rho,A} V + A \Delta_T = S_{\rho,A} \Sigma_{\rho,A} V + A \Delta_T$, and so the matrix $Q_S = A Q_T$ is an approximate matrix basis $S_{\rho,A} U$ for the left singular space $\mathbb{S}_{\rho,A}$ within the error norm bound $\|\Delta_S\| \leq \|A\| \|\Delta_T\|$. Furthermore we can compute the matrix $Q_S^T A Q_T = U^T \Sigma_{\rho,A} V + \Delta_\Sigma$ where $\Delta_\Sigma = \Delta_S^T A Q_T + Q_S^T A \Delta_T - \Delta_S^T A \Delta_T$, and so $\frac{\|\Delta_\Sigma\|}{\|A\|} \leq \|\Delta_S\| + \|\Delta_T\| + \|\Delta_S\| \|\Delta_T\|$. Then the singular values of the $\rho \times \rho$ matrix $Q_S^T A Q_T$ approximate those of the matrix A .

2.4 Oversampling and compression

If we know numerical rank ρ of the input matrix A , we can apply Algorithm 2.1 or 3.1+, for $\rho_+ = \rho$. Otherwise we can compute ρ by applying Algorithm 2.1 or 3.1+ in a binary search process. Indeed, let X denote the output matrix of the algorithm. Then the norm $\|A Q Q^T - A\|$ has order of $\sigma_{\rho+1}(A)$ for $Q = Q(X)$ if $\rho_+ \geq \rho$ (cf. Theorems 2.1 and 2.2), but is at least $\sigma_\rho(A)$ if $\rho_+ < \rho$.

Alternatively, having applied Algorithm 2.1 or 3.1+, for $\rho_+ > \rho$, we can compress the $n \times \rho_+$ output matrix X into $n \times \rho$ orthogonal matrix by means of computing a rank-revealing QR factorization, a UTV factorization, or SVD of the matrix X (see [GL13, Section 5.4] and [S98, Section 5.4] for these factorizations). Such computations are relatively inexpensive if $\rho_+ \ll \min\{m, n\}$, and are routine in the extension of the algorithm to low-rank approximation of the matrix A .

For the task of the approximation of the singular space $\mathbb{T}_{\rho,A}$, however, estimated approximation error norms of these computations are a little larger than $\nu_{n,\rho_+} \sigma_{\rho+1}$, even where we compute the matrix $S_{\rho,X}$ of the ρ leading left singular vectors of the matrix $X = A^T H$ and output it as an approximate matrix basis for the space $\mathbb{T}_{\rho,A}$. Here are some relevant estimates.

Theorem 2.3. *Under the assumptions of Theorem 2.2, write*

$$\phi = \sqrt{n - \rho} \sigma_{\rho+1}(A) \nu_{F,n,\rho_+} \|(A_\rho^T H)^+\|. \quad (2.5)$$

Let the matrix $A_\rho^T H$ have full rank ρ and let $\phi \geq 1$. Then the $n \times \rho$ orthogonal matrix $S_{A_\rho^T H}$ of the ρ leading left singular vectors of the matrix $A_\rho^T H$ approximates a matrix basis of the leading singular space $\mathbb{T}_{\rho,A}$ of the matrix A within the Frobenius error norm 4ϕ .

Proof. Equation (2.4) implies that $\mathcal{R}(T_{\rho,A}) = \mathcal{R}(S_{A_\rho^T H})$. Recall that $A^T H = A_\rho^T H + \bar{A}_\rho^T H$ and combine the upper bound (2.4) on the norm $\|\bar{A}_\rho^T H\|$ with [GL13, Theorem 8.6.5] where $E = \bar{A}_\rho^T H$ and A is replaced by $A_\rho^T H$ (which implies that $\delta = \frac{1}{\|(A_\rho^T H)^+\|}$ in that theorem). \square

Theorem 2.4. *Under the assumptions of Theorem 2.2, it holds that*

$$\|(A_\rho^T H)^+\| \leq \frac{\nu_{\rho,\rho_+}^+}{\sigma_\rho(A)}.$$

Proof. Recall that $A_\rho^T H = T_{\rho,A} \Sigma_{\rho,A} B$ for $B \in \mathcal{G}^{\rho \times \rho_+}$ (cf. (2.4)).

Write $F = \Sigma_{\rho,A} B$ and let $F = S_F \Sigma_F T_F^T$ and $B = S_B \Sigma_B T_B^T$ be compact SVDs.

$T_{\rho,A} S_F$ is an orthogonal matrix because S_F is an $\rho \times \rho$ orthogonal matrix.

Now write $S_{A_\rho^T H} = T_{\rho,A} S_F$ and note that $A_\rho^T H = S_{A_\rho^T H} \Sigma_F T_F^T$ is a compact SVD.

Consequently $\|(A_\rho^T H)^+\| = \|F^+\|$.

Furthermore $F = \Sigma_{\rho,A} S_B \Sigma_B T_B^T$ where $\Sigma_{\rho,A}$, S_B , and Σ_B are $\rho \times \rho$ nonsingular matrices.

Therefore $F^+ = T_B \Sigma_B^{-1} S_B^T \Sigma_{\rho,A}^{-1}$, where $\|S_B\| = \|T_B\| = 1$.

It follows that $\|(A_\rho^T H)^+\| = \|F^+\| \leq \|\Sigma_B^{-1}\| \|\Sigma_{\rho,A}^{-1}\| = \frac{\nu_{\rho,\rho_+}^+}{\sigma_\rho(A)}$. \square

The latter two theorems together imply the following corollary.

Corollary 2.1. *Under the assumption of Theorem 2.2, write*

$$\phi_+ = \sqrt{n - \rho} \nu_{F,n,\rho_+} \nu_{\rho,\rho_+}^+ \frac{\sigma_{\rho+1}(A)}{\sigma_\rho(A)}. \quad (2.6)$$

Then, with a probability at least $\text{Probability}\{5\phi_+ \leq 1\}$, the $n \times \rho$ matrix $S_{A_p^T H}$ of the ρ leading left singular vectors of the matrix $A_p^T H$ approximates a matrix basis of the leading singular space $\mathbb{T}_{\rho, A}$ of the matrix A within the Frobenius error norm $4\phi_+$.

Remark 2.4. For $\rho_+ > \rho$, equation (2.6) and Theorems B.2 and B.3 together imply that

$$\mathbb{E}(\phi_+) < e (1 + \sqrt{n} + \sqrt{\rho_+}) \sqrt{n - \rho} \frac{\sigma_{\rho+1}(A)}{\sigma_\rho(A)} \frac{\sqrt{n\rho_+}}{\rho_+ - \rho}, \text{ for } e = 2.71282\dots$$

2.5 Leading singular spaces via the maximum volume

One can alternatively approximate leading singular spaces by applying the algorithm of [GOSTZ10], devised for the approximation of the so called CUR decomposition of a matrix. The algorithm is heuristic, but consistently converges fast according to its extensive tests by the authors.

It accesses only a small fraction of the entries of the input matrix. This makes it particularly efficient for sparse matrices. The algorithm interchanges rows and columns of an input matrix, destroying Toeplitz-like, Hankel-like, and even Vandermonde-like matrix structures, but one can fix this deficiency by means of the back and forth transition to Cauchy-like matrices [P15], whose structure is invariant in row and column interchange.

The algorithm relies on the following result where we write $v_\rho(M) = \max_X |\det(X)|$ with the maximum over all $\rho \times \rho$ submatrices X of a matrix M , and we call $v_\rho(M)$ the *maximal volume* of all $\rho \times \rho$ submatrices of the matrix M .

Theorem 2.5. [GT01, Corollary 2.3]. Let an $n \times m$ matrix $A^T = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ have a nonsingular $\rho \times \rho$ leading block A_{11} . Write $\nu = \frac{v_\rho(A)}{|\det A_{11}|}$, $C = \begin{pmatrix} A_{11} \\ A_{21} \end{pmatrix}$, and $R = (A_{11} \mid A_{12})$ and let $\|\cdot\|_C$ denote the element-wise (Chebyshev) norm, $\|M\| \leq \sqrt{mn} \|M\|_C$ for a matrix $M \in \mathbb{R}^{m \times n}$. Then

$$\|A - CA_{11}^{-1}R\|_C \leq (\rho + 1)\sigma_{\rho+1}(A)\nu.$$

By virtue of the theorem, the rank- ρ matrix $CA_{11}^{-1}R$ approximates the matrix A within a factor of $(\rho + 1)\nu \sqrt{mn}$ from the optimal error bound $\sigma_{\rho+1}(A)$. ($CA_{11}^{-1}R$ is a CUR decomposition if the matrices A_{11} and $U = A_{11}^{-1}$ are unitary.)

In the authors' tests, the iterative algorithm of [GOSTZ10] has consistently produced $\rho \times \rho$ submatrices of the matrix A that have reasonably bounded ratios ν . This work is linked to our study because a nearly optimal rank- ρ approximation $CA_{11}^{-1}R$ to the matrix A induces close approximations by the matrices C and CA_{11}^{-1} to $n \times \rho$ matrix bases of the leading singular space \mathbb{T}_{ρ, A^T} .

3 Approximation of the Trailing Singular Spaces

3.1 The basic theorems

The following results from [PQ10] and [PQ12] are basic for the approximation of the trailing singular space $\mathbb{T}_{A, \rho}$. We assume that we have already computed the numerical rank ρ , e.g., by applying Algorithms 2.1 or 3.1+ (cf. Remark 2.1).

Theorem 3.1. Suppose that $A \in \mathbb{R}^{m \times n}$, $V \in \mathbb{R}^{n \times s}$, $\hat{K} = \begin{pmatrix} V^T \\ A \end{pmatrix}$, $\text{rank}(V) = s$, $\text{rank}(\hat{K}) = n$, $m \geq n$. Write $\hat{Y} = \hat{K}^{(I)} \begin{pmatrix} I_s \\ O_{m, s} \end{pmatrix}$. Then

- (a) $\mathcal{N}(A) \subseteq \mathcal{R}(\hat{Y})$,
- (b) $\mathcal{N}(A) = \mathcal{R}(\hat{Y})$ if $s + \text{rank}(A) = n$,
- (c) $\mathcal{N}(A) = \mathcal{R}(\hat{Y}\hat{Z})$ if $\mathcal{R}(\hat{Z}) = \mathcal{N}(A\hat{Y})$.

Proof. See [PQ12, Correctness proof of Algorithm 6.1]. □

Theorem 3.2. Suppose that $A \in \mathbb{R}^{m \times n}$, $U \in \mathbb{R}^{m \times q}$, $V \in \mathbb{R}^{n \times s}$, $W \in \mathbb{R}^{s \times q}$, $K = \begin{pmatrix} W & V^T \\ U & A \end{pmatrix}$,

$\text{rank}(W) = q \geq \text{nul}(A)$, $\text{rank}(K) = n + q$, $m \geq n$. Write $\bar{Y} = (O_{n,q} \mid I_n)K^{(I)} \begin{pmatrix} O_{s,q} \\ U \end{pmatrix}$. Then

- (a) $\mathcal{N}(A) \subseteq \mathcal{R}(\bar{Y})$,
- (b) $\mathcal{N}(A) = \mathcal{R}(\bar{Y})$ if $\text{rank}(U) + \text{rank}(A) = n$,
- (c) $\mathcal{N}(A) = \mathcal{R}(\bar{Y}\bar{Z})$ if $\mathcal{R}(\bar{Z}) = \mathcal{N}(A\bar{Y})$.

Proof. See [PQ12, Theorems 11.2 and 11.3]. □

Theorem 3.3. [PQ10, Theorem 3.1 and Corollary 3.1]. Suppose a matrix $A \in \mathbb{R}^{m \times n}$ has rank ρ , $U \in \mathbb{R}^{m \times r}$, $V \in \mathbb{R}^{n \times r}$, and the matrix $C = A + UV^T$ has full rank n . Write $Y = C^{(I)}U$. Then

- (a) $\mathcal{N}(A) \subseteq \mathcal{R}(Y)$ and $r \geq n - \rho$,
- (b) $\mathcal{N}(A) = \mathcal{R}(Y)$ if $r + \rho = n$,
- (c) $\mathcal{N}(A) = \mathcal{R}(YZ)$ if $\mathcal{R}(Z) = \mathcal{N}(AY)$.

Remark 3.1. Given a matrix A and its numerical rank ρ , set to zero all but the ρ largest singular values of the matrix A and arrive at a matrix $A - E$ of rank ρ such that $\|E\| = \sigma_{\rho+1}(A)$. By virtue of our next theorem, the matrix $T_{A,\rho}$ approximates a nmb of a matrix $A - E$ of rank ρ within the norm in $O(\sigma_{\rho+1}(A))$. Therefore $\text{nmb}(A - E)$ can serve as an approximate basis for the trailing singular space $\mathbb{T}_{A,\rho}$, and we can approximate a basis for $\mathbb{T}_{A,\rho}$ within $O(\sigma_{\rho+1}(A))$ by applying the expressions of Theorems 3.1–3.3 to the matrix A rather than to $A - E$ as long as the auxiliary matrices \hat{K} , K and C in these theorems (i) have full rank and (ii) are well-conditioned. For Gaussian matrices U , V , and W , property (i) above follows with probability 1 by virtue of Theorem B.1, and in Sections 4–6 we specify our probability bounds close to 1 with which property (ii) holds.

Theorem 3.4. Suppose that $m \geq n$, an $m \times n$ matrix A has numerical rank $\rho = n - r$, and the matrices C , K , \hat{K} of Theorems 3.1–3.3 have full rank and are well-conditioned. Define the matrices Y , \bar{Y} , and \hat{Y} by the expressions of Theorems 3.1–3.3. Then there exist three orthogonal $r \times r$ matrices X , Z , and \hat{Z} and a scalar c independent of A , U , V , W , m , n and ρ such that

- (i) $\|Q(Y)X - T_{A,\rho}\| \leq c\sigma_{\rho+1}(A)\|U\|$,
- (ii) $\|Q(\bar{Y})Z - T_{A,\rho}\| \leq c\sigma_{\rho+1}(A)\|\bar{Y}\|$,
- (iii) $\|Q(\hat{Y})\hat{Z} - T_{A,\rho}\| \leq c\sigma_{\rho+1}(A)\|\hat{Y}\|$.

Proof. Apply Theorem 3.3 to the matrix $A - E$ of Remark 3.1 such that $\text{rank}(A - E) = \rho$ and $\|E\| = \sigma_{\rho+1}(A)$. Deduce that $T_{A-E,\rho} = Q((C - E)^+U)X$, for $C = A + UV^T$ and an orthogonal $r \times r$ matrix X , and note that the norm $\|(C - E)^+\|$ is not large because the matrix C has full rank and is well-conditioned. In order to prove part (i), it remains to deduce from Theorem A.3 that $\|Q((C - E)^+U) - Q(C^+U)\| = O(\sigma_{\rho+1}(A)\|U\|)$ and $\|T_{A-E,\rho} - T_{A,\rho}Q\| = O(\sigma_{\rho+1}(A))$. □

Similarly we prove parts (ii) and (iii).

3.2 Randomized approximation of a trailing singular space

Assume that $m \geq n$ and we are given an $m \times n$ matrix A and its numerical rank $\rho = n - r$ and seek an approximate basis for the trailing singular space $\mathbb{T}_{A,\rho}$. This can be also viewed as the search for approximate solution of the homogeneous linear system $Az = \mathbf{0}$.

We can compute at first an approximate matrix basis B for the leading singular space $\mathbb{T}_{A,\rho}$, by applying randomized Algorithm 2.1 or 3.1+ (which involve $n\rho_+$ random parameters and $(2n - 1)\rho_+$ flops or $n + \rho_+$ parameters and $O(mn \log(\rho_+ + n\rho_+^2))$ flops, respectively), and then an approximate matrix basis $\text{nmb}(B)$ for the trailing singular space $\mathbb{T}_{A,\rho}$. We refer to these algorithms as **Algorithms 3.1t** and **3.1t+**.

At the stage of computing a $\text{nmb}(B)$, we can apply the algorithms supporting Theorems 3.1–3.4, but in this application to $m \times \rho$ matrix AH , for $\rho < m$, they are superseded by [PQ12, Algorithm 4.1], which generates an $n \times n$ Gaussian multiplier and then performs about $2(n + \rho)n\rho$ flops.

If we apply a SRFT multiplier of Appendix C instead of the Gaussian one, then we would generate only $n + \rho_+$ random values for ρ_+ of order $(\rho + \log(n)) \log(\rho)$ and would perform $O((\rho_+^2 + \log(n))n)$

flops, but the estimated failure probability would increase from $3/p^p$ to the order $1/\rho$ (see Remark C.2 and Section 6.2).

Next we describe some randomized alternatives for direct approximation of a basis for the trailing singular space $\mathbb{T}_{A,\rho}$, which rely on Theorems 3.1–3.4 and Remark 3.1. They can fail like Algorithms 2.1 and 3.1+ and can run into numerical problems, but in both cases only with a probability close to 0 (according to our estimates in Sections 4–6) and never in our extensive tests. Moreover, we can detect the failure by following the recipe of Remark 2.1.

Algorithm 3.1. An approximate basis for the trailing singular space by using randomized preprocessing.

INPUT: A normalized matrix $A \in \mathbb{R}^{m \times n}$ for $m \geq n$, its numerical rank $\rho = n - r$, possibly computed by Algorithm 2.1 or 3.1+ (cf. Remark 2.1), and a tolerance value $\tau \gg \sigma_{\rho+1}(A)$.

OUTPUT: An approximate matrix basis B of the trailing singular space $\mathbb{T}_{A,\rho}$ within a relative error norm bound τ .

INITIALIZATION: Choose one of Theorems 3.1–3.3 and generate the auxiliary Gaussian matrices U , U and V , or U , V , and W involved into it.

COMPUTATIONS:

1. Compute an approximate orthogonal matrix basis X for the trailing singular space $\mathbb{T}_{A,\rho}$ by setting $X = Y$, $X = \bar{Y}$, or $X = \hat{Y}$ and using the expression of the selected theorem. Compute the matrix AX .
2. Output $B = X$ and stop if $\|AX\| \leq \tau\|A\|$. Otherwise output FAILURE and stop.

We have three options for proceeding with any of three Theorems 3.1–3.3 and thus arrive at the three variants of the algorithm. Hereafter we refer to them as **Algorithms 4.1.1**, **4.1.2**, and **4.1.3**.

The algorithms generate nr , $(m+n+r)r$, and $(m+n)r$ i.i.d. Gaussian parameters, respectively, and then perform order of $(m+r)n^2$, $(m+r)(n+r)^2$, and $(n+r)mn$ flops, respectively.

By choosing SRFT matrices U , V and W , we can decrease the number of random parameters involved to $m+r_+$, $m+n+r_+$, and $m+n+r_+$, respectively, for r_+ of order $(r+\log(n))\log(r)$, $(r+\log(m+n))\log(r)$, and $(r+\log(m+n))\log(r)$, respectively, and then the order of the estimated upper bound on the failure probability would increase from $3/p^p$, for $p = r_+ - r$, to the order $1/r$.

Remark 3.2. One can compute nmbs, matrix bases, and approximate matrix bases of the left trailing singular spaces of a matrix A as the nmbs, matrix bases and approximate matrix bases of the trailing singular spaces of the transposed matrix A^T or sometimes by simpler means (see Remark 2.3).

Remark 3.3. In the case where $m = n$ the computations are simplified and stabilized numerically. We can reduce to this case the computation for a rectangular matrix A , e.g., by observing that

- $\mathcal{N}(A) = \mathcal{N}(A^T A)$,
- $\mathcal{N}(A) = \mathcal{N}(B^T A)$ if $A, B \in \mathbb{R}^{m \times n}$ and if the matrix B has full rank $m \leq n$,
- $(A \mid O_{m,m-n})\mathbf{u} = \mathbf{0}_m$ if and only if $A\hat{\mathbf{u}} = \mathbf{0}_m$ provided that $m \geq n$ and $\hat{\mathbf{u}} = (I_n \mid O_{n,m-n})\mathbf{u}$,
- $(A^T \mid O_{n,m-n})\mathbf{v} = \mathbf{0}_n$ if and only if $\hat{\mathbf{v}} = \mathbf{0}_n^T$ provided that $m < n$ and $\hat{\mathbf{v}} = (I_m \mid O_{n-m,m})\mathbf{v}$.

Furthermore, here is an alternative option. Represent an $m \times n$ matrix A for $m > n$ as a block vector $A = (B_1^T \mid B_2^T \mid \dots \mid B_h^T)^T$ for $k_i \times n$ blocks B_i , $i = 1, \dots, h$, and $\sum_{i=1}^h k_i = m$. Note that $\mathcal{N}(A) = \cap_{i=1}^h \mathcal{N}(B_i)$ and apply [GL13, Theorem 6.4.1] to compute the intersection of null spaces.

Remark 3.4. Recursive randomized approximation of the bases of singular spaces. Given a matrix A and two small positive values η and $\eta' < \eta$, suppose that we have computed the integers $\rho = \text{rank}_\eta(A)$ and $\rho' = \text{rank}_{\eta'}(A)$, by applying Algorithm 2.1 or 3.1+, as well as an approximate basis $Y = Y_\eta$ for the trailing singular space $\mathbb{T}_{A,\rho}$, by applying Algorithm 3.1t, 3.1t+, 4.1.1, 4.1.2, or 4.1.3. Now suppose that we seek an approximate matrix basis $Y' = Y_{\eta'}$ for the trailing singular space $\mathbb{T}_{\rho',A}$. Then again we can apply one of these algorithms to the matrix A , but we can apply it to the matrix AY instead, by increasing the precision u of computing to $u' > u$ such that $2^{u'} = O(\sigma_{\rho'+1}(A))$, but decreasing the arithmetic cost by a factor of n/ρ , which is substantial if $\rho \ll n$. Correctness of this recipe follows from Theorems 3.1–3.4, and the approach can be extended recursively.

PART II: Augmentation and Additive Preprocessing

4 Analysis of Randomized Augmentation

Our algorithms of the previous two sections rely on the power of randomized augmentation and additive preprocessing, which we prove in this and the next two sections.

Row and column permutations make no impact on the singular values of a matrix, and so we restrict our next study to western, northern and northwestern augmentation, that is, to appending Gaussian rows on the top of a matrix or Gaussian columns on the left of it. Furthermore, western augmentation for a matrix turns into northern augmentation for its transpose and vice versa, and so it is sufficient to analyze western and northwestern augmentation.

In the next two subsections we prove the same quite reasonable upper bound on the condition numbers of two matrices obtained from the same ill-conditioned matrix by means of western and northwestern augmentation, respectively, but in order to yield this upper bound, the northwestern augmentation requires about twice as many random parameters. Our tests in Section 7 complement these results by clearly showing superior performance of western versus northwestern augmentation as well as versus additive preprocessing. Some potential applications, however, may require northwestern rather than western augmentation (see, e.g., the end of Section 8).

4.1 Analysis of western and northern augmentation

Assumption 1. We will simplify our presentation by omitting the restriction "with probability 1". For example, by saying that a random matrix A has full rank or showing an estimate for the norm $\|A^+\|$, we will assume by default (although will not state explicitly) that these property or estimate hold with probability 1.

Theorem 4.1. (Cf. Remark 4.1 and Definition 2.1.) Assume that an $m \times n$ matrix A is normalized and has numerical rank ρ . Define its randomized western augmentation by the map $A \Rightarrow K = (U \mid A)$ for $U \in \mathcal{G}^{m \times q}$. Then

$$\|K\| \leq \|A\| + \|U\| = 1 + \nu_{m,q}, \quad (4.1)$$

for the random variable $\nu_{m,q}$ defined in Section 2.3 and Appendix B. Furthermore

- (i) the matrix K is rank deficient or ill-conditioned if $q + \rho < l = \min\{m, n\}$.
- (ii) Otherwise it has full rank and
- (iii) satisfies the following bound,

$$\|K^+\| \leq n_{m,q,\rho,A}^+ = \max\{1, \nu_{m-\rho,q}^+\} \frac{1 + \nu_{\rho,m-\rho}}{\sigma_\rho(A)}. \quad (4.2)$$

Proof. Readily verify (4.1) and part (i). Deduce part (ii) from Theorem B.1.

It remains to prove bound (4.2) provided that $l \leq q + \rho$.

With no loss of generality, we can replace the matrix A by the diagonal matrix Σ_A of its singular values, that is, we can write

$$A = \Sigma_A = \text{diag}(\Sigma_\rho, \Sigma'_{m-\rho, n-\rho}) \text{ and } K = \begin{pmatrix} U_0 & \Sigma_\rho & O_{\rho, n-\rho} \\ \bar{U} & O_{m-\rho, \rho} & \Sigma'_{m-\rho, n-\rho} \end{pmatrix}$$

where $\|\Sigma'_{m-\rho, n-\rho}\| = \sigma_{\rho+1}(A)$, $\Sigma_\rho = \Sigma_{\rho, A} = \text{diag}(\sigma_j(A))_{j=1}^\rho$, $U_0 \in \mathcal{G}^{\rho \times q}$, and $\bar{U} \in \mathcal{G}^{(m-\rho) \times q}$. Indeed, we arrive at these equations by applying the orthogonal map $K \rightarrow S_A^T K \text{diag}(I_q, T_A)$, which also induces the map $A \rightarrow S_A^T A T_A = \Sigma_A$. Here S_A and T_A are the matrices of the singular vectors in SVD $A = S_A \Sigma_A T_A^T$, and we note that $S_A^T U \text{diag}(I_q, T_A) \in \mathcal{G}^{m \times q}$ by virtue of Lemma B.1 and that the map preserves all singular values of the matrix K . We call such maps *Gaussian diagonalization*.

Furthermore with no loss of generality we can assume that $n = \rho = l \leq m$ and that

$$K = \begin{pmatrix} U_0 & \Sigma_\rho \\ \bar{U} & O_{m-\rho, \rho} \end{pmatrix} \in \mathbb{R}^{m \times (n+q)}$$

because the $n - q$ rightmost columns of the matrix K are filled with zeros, and we could just delete them. Note that Theorem B.1 and Assumption 1 together imply that the $(m - \rho) \times q$ matrix \bar{U} has full rank, and so $\text{rank}(K) = m$ because $q + \rho \geq m$.

Then again apply Gaussian diagonalization by writing

$$\hat{K} = \text{diag}(I_\rho, S_{\bar{U}}^T) K \text{diag}(T_{\bar{U}}^T, I_\rho) = \begin{pmatrix} U_{00} & U_{01} & \Sigma_\rho \\ \Sigma'_{\bar{U}} & O_{m-\rho, q+\rho-m} & O_{m-\rho, \rho} \end{pmatrix}$$

where $\bar{U} = S_{\bar{U}} \Sigma_{\bar{U}} T_{\bar{U}}^T$ is SVD, $\Sigma_{\bar{U}} = (\Sigma'_{\bar{U}} \mid O_{m-\rho, q+\rho-m})$, $(U_{00} \mid U_{01}) = U_0 T_{\bar{U}}^T \in \mathcal{G}^{\rho \times q}$ by virtue of Lemma B.1, and $U_{00} \in \mathcal{G}^{\rho \times (m-\rho)}$. Note that $\|K^+\| = \|\hat{K}^+\|$.

The $m \times m$ submatrix

$$\bar{K} = \begin{pmatrix} U_{00} & \Sigma_\rho \\ \Sigma'_{\bar{U}} & O_{m-\rho, \rho} \end{pmatrix}$$

of the matrix \hat{K} , obtained by deleting the submatrix $\begin{pmatrix} U_{01} \\ O_{m-\rho, q+\rho-m} \end{pmatrix}$, is nonsingular by virtue of Theorem B.1 (cf. Assumption 1). Moreover $\|K^+\| = \|\hat{K}^+\| \leq \|\bar{K}^{-1}\|$ by virtue of Lemma A.3.

Now observe that

$$\begin{aligned} \bar{K}^{-1} &= \begin{pmatrix} O_{m-\rho, \rho} & (\Sigma'_{\bar{U}})^{-1} \\ \Sigma_\rho^{-1} & -\Sigma_\rho^{-1} U_{00} (\Sigma'_{\bar{U}})^{-1} \end{pmatrix} = \text{diag}(I_\rho, \Sigma_\rho^{-1}) \begin{pmatrix} O_{m-\rho, \rho} & I_\rho \\ I_{m-\rho, m-\rho} & U_{00} \end{pmatrix} \text{diag}(I_\rho, \Sigma'_{\bar{U}})^{-1}, \\ \left\| \begin{pmatrix} O_{m-\rho, \rho} & I_\rho \\ I_{m-\rho, m-\rho} & U_{00} \end{pmatrix} \right\| &\leq 1 + \|U_{00}\| = 1 + \nu_{\rho, m-\rho}, \\ \|\text{diag}(I_\rho, (\Sigma'_{\bar{U}})^{-1})\| &= \max\{1, \|(\Sigma'_{\bar{U}})^{-1}\|\} = \max\{1, \|\bar{U}^+\|\} = \max\{1, \nu_{m-\rho, q}^+\}, \\ \|\text{diag}(I_\rho, \Sigma_\rho^{-1})\| &= \max\{1, \|\Sigma_\rho^{-1}\|\} = \frac{1}{\sigma_\rho(A)}. \end{aligned}$$

The latter equation follows because $\sigma_\rho(A) \leq \|A\|$ and because $\|A\| = 1$ by assumption.

Combine the above observations with the bound $\|K^+\| \leq \|\bar{K}^{-1}\|$ and obtain (4.2). \square

Next we combine Theorems 4.1, B.2, and B.3 and obtain the following bounds on the expected values of the norms $\|K\|$ and $\|K^+\|$ (excluding the case where $q + \rho = m$ and the auxiliary random variable $\nu_{m-\rho, q}^+$ of (6.5) has no expected value).

Corollary 4.1. *Under the assumptions of Theorem 4.1, it holds that*

$$\mathbb{E}(\|K\|) < 2 + \sqrt{m} + \sqrt{q},$$

and if $q + \rho > l = \min\{m, n\}$, then

$$\mathbb{E}(\|K^+\|) < \frac{2 + \sqrt{\rho} + \sqrt{l - \rho}}{\sigma_\rho(A)} \max\left\{1, \frac{e\sqrt{(l - \rho)}}{q + \rho - l}\right\}, \text{ for } e = 2.71828 \dots \quad (4.3)$$

Remark 4.1. Theorem 4.1 and the corollary show that the western augmentation is likely to output a well-conditioned matrix K , particularly if the ratio $\frac{e\sqrt{(l-\rho)}}{q+\rho-l}$ is small. We can partly control this ratio by choosing the integer parameter q . If we decrease the ratio below 1, then it would hold that $\mathbb{E}(\|K^+\|) < \frac{2+\sqrt{\rho}+\sqrt{l-\rho}}{\sigma_\rho(A)}$, where the value $\sigma_\rho(A)$ is not small by assumption.

By applying Theorem 4.1 and the corollary to the matrix A^T , we can extend them to northern augmentation, that is, to appending a Gaussian block of $s \geq n - \rho$ rows on the top of the matrix A .

4.2 Analysis of northwestern augmentation

Theorem 4.2. Assume that an $m \times n$ matrix A is normalized and has numerical rank ρ . Define its randomized northwestern augmentation by the map

$$A \rightarrow K = \begin{pmatrix} W & V^T \\ U & A \end{pmatrix} \quad (4.4)$$

where $W \in \mathcal{G}^{s \times q}$, $U \in \mathcal{G}^{m \times q}$, $V \in \mathcal{G}^{n \times q}$, and the matrices U , V , and W are filled with i.i.d. Gaussian variables. Then

$$\|K\| \leq \|A\| + \min\{\|U\| + \|(W \mid V^T)\|, \|V\| + \left\| \begin{pmatrix} W \\ U \end{pmatrix} \right\|\} = 1 + \min\{\nu_{m,q} + \nu_{s,n+q}, \nu_{s,n} + \nu_{m+s,q}\}. \quad (4.5)$$

Furthermore

- (i) the matrix K is rank deficient or ill-conditioned if $q + \rho < m$ and if $s + \rho < n$.
- (ii) Otherwise it has full rank and
- (iii) satisfies the following bounds,

$$\|K^+\| \leq n_{m,q,\rho,A}^+, \text{ for } q + \rho \geq m, \text{ and} \quad (4.6)$$

$$\|K^+\| \leq n_{n,s,\rho,A^T}^+, \text{ for } s + \rho \geq n, \quad (4.7)$$

where the random variables $n_{m,q,\rho,A}^+$ and n_{n,s,ρ,A^T}^+ are defined by equation (4.2).

Proof. Readily verify (4.1) and part (i). Deduce part (ii) from Theorem B.1. It remains to prove bounds (4.6) and (4.7).

Define western augmentation

$$\hat{A} \rightarrow K = (\hat{U} \mid \hat{A}),$$

for K of (4.4),

$$\hat{U} = \begin{pmatrix} W^T \\ V \end{pmatrix} \text{ and } \hat{A} = \begin{pmatrix} U^T \\ A^T \end{pmatrix}.$$

Replace the matrix A by \hat{A} and the integers m , n , l , q , and ρ by $\hat{m} = n + q$, $\hat{n} = m$, $\hat{l} = \min\{n + q, m\}$, $\hat{q} = s$, and $\hat{\rho} = m$, respectively. Note that $n + q \geq q + \rho \geq m$, and so $\hat{l} = m$ and $\hat{\rho} + \hat{q} = m + s \geq \hat{l} = m$, which implies extension of bound (4.2) to this case. Obtain (4.6) because $\sigma_{\hat{\rho}}(\hat{A}) = \|\hat{A}^+\| = n_{m,q,\rho,A}^+$.

Likewise define western augmentation

$$\bar{A} \rightarrow K = (\bar{U} \mid \bar{A}),$$

for K of (4.4),

$$\bar{U} = \begin{pmatrix} W \\ U \end{pmatrix} \text{ and } \bar{A} = \begin{pmatrix} V^T \\ A \end{pmatrix}.$$

Replace the matrix A by \bar{A} and the integers m , n , l , q , and ρ by $\bar{m} = m + s$, $\bar{n} = n$, $\bar{l} = \min\{n, m + s\}$, $\bar{q} = q$, and $\bar{\rho} = \min\{\rho + s, n\}$, respectively. Note that $m + s \geq q + \rho \geq n$, and so $\bar{l} = n$ and $\bar{\rho} + \bar{s} = \bar{\rho} + q \geq \bar{l} = n$, which implies extension of bound (4.2) to this case. Obtain (4.7) because $\sigma_{\bar{\rho}}(\bar{A}) = \|\bar{A}^+\| = n_{l,s,\rho,A}^+$. \square

The theorem indicates that appending Gaussian rows in addition to Gaussian columns as well as appending Gaussian columns in addition to Gaussian rows is not likely to increase the norm of the Moore-Penrose generalized inverse of a normalized matrix.

By combining Theorems 4.2, B.2, and B.3, we obtain the following bounds.

Corollary 4.2. *Keep the assumptions of Theorem 4.2; in particular keep the definitions of the integers \tilde{l} , $\hat{\rho}$, \bar{l} , and $\bar{\rho}$. Write $e = 2.71828 \dots$. Then*

$$\mathbb{E}(\|K\|) < 3 + \sqrt{q} + \sqrt{s} + \min\{\sqrt{m} + \sqrt{n+q}, \sqrt{n} + \sqrt{m+s}\}$$

and $\mathbb{E}(\|K^+\|)$ satisfies either bound (4.3) if $q + \rho > m$ or the same bound but with the integer parameter s replacing q if $s + \rho > n$.

4.3 Analysis of weakly randomized northwestern augmentation

In the next section we analyze randomized additive preprocessing by linking it to northwestern augmentation (4.4), for $m = n$ and $r = q = s = n - \rho$, which we modify by choosing $W = I_r$ rather than $W \in \mathcal{G}^{m \times n}$ and where we allow the Gaussian matrices U and V to depend on one another and even to share all their entries. We call such northwestern augmentation *weakly randomized*. Next we extend to it Theorem 4.2.

Theorem 4.3. *Suppose that an $n \times n$ matrix A is normalized and has numerical rank ρ , K is the matrix of (4.4), $W = I_r$, and $U, V \in \mathcal{G}^{n \times r}$ where $r = n - \rho$. Then*

$$\|K\| \leq \|A\| + \|U\| + \|V\| + \|W\| = 2 + 2\nu_{r,n},$$

the matrix K is nonsingular, and

$$\|K^{-1}\| \leq 1.5\bar{n}, \text{ for } \bar{n} = (1 + \nu_{\rho,r}) \left(1 + \frac{\nu_{\rho,r}}{\sigma_\rho(A)}\right) \max\{1, \frac{\nu_{r,r}^+}{\sigma_\rho(A)}\} \max\{1, \nu_{r,r}^+\}. \quad (4.8)$$

Proof. We only estimate the norm $\|K^{-1}\|$. At first let $\text{nrnk}(A) = \text{rank}(A) = \rho$ and then reduce our study to the case where $A = \Sigma_A = \text{diag}(\Sigma_{\rho,A}, O_{r,r})$ by combining Gaussian diagonalization $K \rightarrow \text{diag}(I_r, S_A^T) K \text{diag}(I_r, T_A)$ and Lemma B.1. Write

$$K = \begin{pmatrix} I_r & V_0^T & V_1^T \\ U_0 & \Sigma_\rho & O_{\rho,r} \\ U_1 & O_{r,\rho} & O_{r,r} \end{pmatrix}$$

where $U_0, V_0 \in \mathcal{G}^{\rho \times r}$, $U_1, V_1 \in \mathcal{G}^{r \times r}$, and the matrix K is nonsingular (cf. Theorem B.1 and Assumption 1). Express the inverse K^{-1} as follows,

$$K^{-1} = \begin{pmatrix} O_{r,r} & O_{r,\rho} & U_1^{-1} \\ O_{\rho,r} & \Sigma_\rho^{-1} & -\Sigma_\rho^{-1} U_0 U_1^{-1} \\ V_1^{-T} & -V_1^{-T} V_0^T \Sigma_\rho^{-1} & V_1^{-T} (I_r - V_0^T \Sigma_\rho^{-1} U_0) U_1^{-1} \end{pmatrix} =$$

$$\text{diag}(I_r, \Sigma_\rho^{-1}, V_1^{-T}) \left(I_{n+r} + \text{diag}(O_{n,n}, I_r) - \text{diag}(O_{r,r}, F_\rho) \right) \text{diag}(I_n, U_1^{-1})$$

where

$$F_\rho = \begin{pmatrix} O_{\rho,\rho} & U_0 \\ V_0^T \Sigma_\rho^{-1} & V_0^T \Sigma_\rho^{-1} U_0 \end{pmatrix} = \text{diag}(I_\rho, V_0^T \Sigma_\rho^{-1}) \text{diag}(O_{\rho,\rho}, I_r) \text{diag}(I_\rho, U_0).$$

Combine the above expressions and deduce that $\|K^{-1}\| \leq \bar{n}$, for \bar{n} of equation (4.8).

This is the upper bound of Theorem 4.3 decreased by a factor of 1.5.

By sacrificing this factor, we relax the assumption that $\text{nrnk}(A) = \text{rank}(A)$.

Namely, without this assumption, our previous argument implies that

$$K = \begin{pmatrix} I_r & V_0^T & V_1^T \\ U_0 & \Sigma_\rho & O_{\rho,r} \\ U_1 & O_{r,\rho} & \Sigma'_{r,r} \end{pmatrix}$$

where the value $\|\Sigma'_{r,r}\| = \sigma_{\rho+1}(A)$ is small since $\text{nrnk}(A) = \rho$. Apply Theorem A.2 for $\theta < 1/3$ and obtain that $\|K^{-1}\| < 1.5\bar{n}$. \square

Remark 4.2. Our upper bound on the norm $\|K^+\|$ involves the factor $(\nu_{r,r}^+)^2$. For larger integers r , this makes the bound inferior to those of the previous two subsections: the random variable $\nu_{r,r}^+$ has no expected value; its upper bound in part 2 of Theorem B.3, although meaningful, is inferior to the bounds on the random variables $\nu_{i,j}$ and $\nu_{r,s}^+$ as long as the integer $|s - r|$ is not close to 0.

5 Analysis of Randomized Additive Preprocessing

In this section we analyze randomized additive preprocessing

$$A \rightarrow C = A + UV^T \text{ for } A, C \in \mathbb{R}^{n \times n} \text{ and } U, V \in \mathcal{G}^{n \times r}, \quad (5.1)$$

where the entries of the matrices U and V may depend on each other, and we even allow $U = V$.

We immediately observe the following properties.

Theorem 5.1. Suppose that A , C , U , and V are four matrices of (5.1). Then

$$\|C\| \leq \|A\| + \|U\| \|V\| \leq \|A\| + \nu_{n,r}^2, \quad (5.2)$$

the matrix C is nonsingular if and only if $\text{rank}(A) + r \geq n$ (cf. Assumption 1 and Theorem B.1 or [PQ10]), and in this case the matrix C is ill-conditioned if $\text{nrnk}(A) + r < n$.

Next we estimate the norm $\|C^{-1}\|$ provided that $\text{nrnk}(A) + r \geq n$. We do this at first by linking additive preprocessing to augmentation, then directly.

5.1 Estimation of the norm $\|C^{-1}\|$ via a link to augmentation

The following theorem links augmentation (4.4), for $W = I_r$, to additive preprocessing of (5.1).

Theorem 5.2. Suppose that $A \in \mathbb{R}^{n \times n}$, $U, V \in \mathbb{R}^{n \times r}$, $K = \begin{pmatrix} I_r & V^T \\ U & A \end{pmatrix}$, and $C = A + UV^T$.

Write $\hat{U} = \begin{pmatrix} O_{r,n} & I_r \\ I_n & U \end{pmatrix}$, $\hat{V} = \begin{pmatrix} O_{n,r} & I_n \\ I_r & V^T \end{pmatrix}$, $\hat{U}^{-1} = \begin{pmatrix} -U & I_n \\ I_r & O_{r,n} \end{pmatrix}$, $\hat{V}^{-1} = \begin{pmatrix} -V^T & I_r \\ I_n & O_{n,r} \end{pmatrix}$, and $D_{n,r} = \text{diag}(I_n, O_{r,r})$. Then

$$K = \hat{U} \text{diag}(C, I_r) \hat{V}, \quad C = D_{n,r} \hat{U}^{-1} K \hat{V}^{-1} D_{n,r}. \quad (5.3)$$

Furthermore both matrices C and K are singular or nonsingular simultaneously.

They are singular if $r + \text{rank}(A) < n$.

If the matrices C and K are nonsingular, then

$$K^{-1} = \hat{V}^{-1} \text{diag}(C^{-1}, I_r) \hat{U}^{-1}, \quad C^{-1} = D_{n,r} \hat{V} K^{-1} \hat{U} D_{n,r},$$

$$\|C^{-1}\| \leq (1 + \|U\|)(1 + \|V\|)\|K^{-1}\|, \text{ and } \|K^{-1}\| \leq (1 + \|U\|)(1 + \|V\|) \max\{1, \|C^{-1}\|\}.$$

By combining Theorems 4.3 and 5.2 we extend our results for weakly randomized northwestern augmentation of (4.4) to randomized additive preprocessing.

Corollary 5.1. Suppose that A , C , U , and V are matrices of (5.1), $\|A\| = 1$, and $\text{nrnk}(A) + r \geq n$, and so the matrix C is nonsingular (with probability 1) (cf. Theorem 5.1). Define \bar{n} by (4.8). Then

$$\|C^{-1}\| \leq 1.5(1 + \nu_{n,r})^2 \bar{n}.$$

5.2 Direct estimation of the norm $\|C^{-1}\|$

At first we bound the ratio $\frac{\kappa(C)}{\kappa(A)}$ in the case where $\text{rank}(A) + r = n$, then extend the bound to the case where $\text{nrnk}(A) + r = n$ and in the next subsection to the case where $\text{nrnk}(A) + r \geq n$.

Theorem 5.3. *Suppose that $A, S, T \in \mathbb{R}^{n \times n}$ and $U, V \in \mathbb{R}^{n \times r}$ for two positive integers r and n , $r \leq n$, $A = S\Sigma T^T$ is SVD of the matrix A (cf. (2.1)), S and T are square orthogonal matrices, $\Sigma = \text{diag}(\sigma_j)_{j=1}^n$, $\rho = \text{rank}(A) = n - r$, $\sigma_\rho > 0$, and the matrix $C = A + UV^T$ is nonsingular. Towards Gaussian diagonalization of the matrix C , introduce the matrices*

$$S^T U = \begin{pmatrix} \bar{U} \\ U_r \end{pmatrix}, \quad T^T V = \begin{pmatrix} \bar{V} \\ V_r \end{pmatrix}, \quad R_U = \begin{pmatrix} I_\rho & \bar{U} \\ O_{r,\rho} & U_r \end{pmatrix}, \quad R_V = \begin{pmatrix} I_\rho & \bar{V} \\ O_{r,\rho} & V_r \end{pmatrix}, \quad (5.4)$$

where U_r and V_r are $r \times r$ matrices. Then

(a) $R_U \Sigma R_V^T = \Sigma$, $R_U \text{diag}(O_{\rho,\rho}, I_r) R_V^T = S^T U V^T T$, and so

$$C = S R_U D R_V^T T^T, \quad D = \Sigma + \text{diag}(O_{\rho,\rho}, I_r) = \text{diag}(d_j)_{j=1}^n \quad (5.5)$$

where $d_j = \sigma_j$ for $j = 1, \dots, \rho$, $d_j = 1$ for $j = \rho + 1, \dots, n$.

Furthermore suppose that $\|A\| = 1$ and the $r \times r$ matrices U_r and V_r are nonsingular. Write

$$p = \|R_U^{-1}\| \|R_V^{-1}\| \text{ and } f_r = \max\{1, \|U_r^{-1}\|\} \max\{1, \|V_r^{-1}\|\}. \quad (5.6)$$

Then

(b) $1 \leq \frac{\sigma_\rho(A)}{\sigma_n(C)} \leq p$ and

(c) $p \leq (1 + \|U\|)(1 + \|V\|)f_r$.

Proof. Part (a) is readily verified.

Let us prove part (b). Combine the equations $S^{-1} = S^T$, $T^{-1} = T^T$ and (5.5) and obtain $C^{-1} = T R_V^{-T} D^{-1} R_U^{-1} S^T$.

Apply bound (A.1), substitute $\|S^T\| = \|T\| = 1$, and obtain $\|C^{-1}\| \leq \|R_V^{-T}\| \|D^{-1}\| \|R_U^{-1}\|$.

Substitute equations (5.6), $\|D^{-1}\| = \frac{1}{\sigma_\rho(A)}$ (implied by the equations $\|A\| = 1$ and (5.5)), and

$\|C^{-1}\| = \frac{1}{\sigma_n(C)}$ and obtain that $\frac{\sigma_\rho(A)}{\sigma_n(C)} \leq p$.

Next deduce from (5.4) and (5.5) that

$$R_V^{-T} = \begin{pmatrix} I_\rho & O_{\rho,r} \\ -V_r^{-T} \bar{V}^T & V_r^{-T} \end{pmatrix}, \quad D^{-1} = \Sigma^{-1} + \text{diag}(O_{\rho,\rho}, I_r), \quad R_U^{-1} = \begin{pmatrix} I_\rho & -\bar{U} U_r^{-1} \\ O_{r,\rho} & U_r^{-1} \end{pmatrix}.$$

Substitute these expressions into the matrix product $R_V^{-T} D^{-1} R_U^{-1}$ and obtain that $R_V^{-T} D^{-1} R_U^{-1} = \begin{pmatrix} \Sigma^{-1} & X \\ Y & Z \end{pmatrix}$. Consequently $\frac{1}{\sigma_n(C)} = \|C^{-1}\| = \|R_V^{-T} D^{-1} R_U^{-1}\| \geq \|\Sigma^{-1}\| = \frac{1}{\sigma_n(A)}$.

This completes the proof of part (b).

(c) Observe that $R_U^{-1} = \begin{pmatrix} I_\rho & -\bar{U} \\ O & I_r \end{pmatrix} \begin{pmatrix} I_\rho & O \\ O & U_r^{-1} \end{pmatrix}$, $R_V^{-1} = \begin{pmatrix} I_\rho & -\bar{V} \\ O & I_r \end{pmatrix} \begin{pmatrix} I_\rho & O \\ O & V_r^{-1} \end{pmatrix}$, $\|\bar{U}\| \leq \|U\|$ and $\|\bar{V}\| \leq \|V\|$. Then combine these relationships with (5.6). \square

Corollary 5.2. *Suppose that $A \in \mathbb{R}^{n \times n}$ and $U, V \in \mathbb{R}^{n \times r}$ for two positive integers n and r such that $\rho = \text{rank}(A) = n - r$, and $C = A + UV^T$. Then*

$$\|C^+\| \leq (1 + \|U\|)(1 + \|V\|) \max\{1, \|U_r^{-1}\|\} \max\{1, \frac{\|V_r^{-1}\|}{\sigma_n(A)}\}. \quad (5.7)$$

Proof. Equation (5.6) and parts (b) and (c) of Theorem 5.3 together imply (5.7). \square

Corollary 5.3. *Keep the assumptions of Corollary 5.2, but assume that $\text{nrnk}(A) = \rho \leq \text{rank}(A)$ and $U, V \in \mathcal{G}^{n \times r}$. Then*

(i) *the matrix C is nonsingular with probability 1 and*

$$(ii) \|C^{-1}\| \leq 1.5(1 + \nu_{n,r}^2) \max\{1, \nu_{n,r}^+\} \max\{1, \frac{\nu_{r,r}^+}{\sigma_\rho(A)}\}.$$

Proof. Part (i) follows from Theorem B.1.

Next note that U_r and V_r are Gaussian matrices by virtue of Lemma B.1 because $U, V \in \mathcal{G}^{n \times r}$. At first let the matrix A be rank deficient and well-conditioned, such that $\text{nrnk}(A) = \text{rank}(A)$.

Then $\|C^+\| \leq (1 + \nu_{n,r}^2) \max\{1, \nu_{n,r}^+\} \max\{1, \frac{\nu_{r,r}^+}{\sigma_\rho(A)}\}$ by virtue of Corollary 5.2, and part (ii) of Corollary 5.3 follows from Theorems B.2 and B.3.

Finally, as at the end of our proof of Theorem 4.3, apply a small norm perturbation of this matrix and extend this estimate to the general case where $\text{nrnk}(A) = \rho \leq \text{rank}(A)$. \square

Remark 5.1. *The upper bound of the corollary on the norm $\|C^{-1}\|$ is quite reasonable. It is proportional to $\nu_{r,r}^+$, which makes it superior to the bound of Corollary 5.1, proportional to $(\nu_{r,r}^+)^2$ (cf. Remark 4.2). Moreover in our extensive tests the norm $\|C^{-1}\|$ has consistently stayed at a substantially lower level, namely at the level of the norms $\|K^+\|$ of the matrices generated from the same input matrices A by means of northwestern augmentation.*

5.3 Extension to additive preprocessing of rectangular matrices with multipliers of larger sizes

We have bounded the condition number $\kappa(C)$ of the matrix $C = A + UV^T$ in two ways – by linking additive preprocessing to augmentation and directly – and in both cases, under the assumptions that $m = n$ and $\rho = \text{nrnk}(A) > n - r$. Next we remove both of these assumptions, at the price of increasing our upper bound on the norm $\|C^+\|$ well above the square of the bounds of Corollaries 5.1 and 5.3. Such an increase may be due to some technicalities of our proof, such as application of the Sherman—Morrison—Woodbury formula³ (cf. [GL13, page 65])

$$C^{-1} = (\Sigma_{C_-} + \bar{U}\bar{V}^T)^{-1} = \Sigma_{C_-}^{-1} - \Sigma_{C_-}^{-1}\bar{U}(I_{r-r_-} + \bar{V}^T\Sigma_{C_-}^{-1}\bar{U})^{-1}\bar{V}^T\Sigma_{C_-}^{-1}, \quad (5.8)$$

and this poses a research challenge of improving our estimates.

Theorem 5.4. *Keep the assumptions of Corollary 5.3, but allow that $\rho = \text{nrnk}(A) > n - r$. Then*

$$\|C^{-1}\| \leq \nu_{n,n}^+ \nu_n^+ \text{ if } r \geq 2n - \rho \quad (5.9)$$

where ν_n and $\nu_{n,n}$ are bounded in (2.3) and in part 2 of Theorem B.3.

If $n - \rho < r < 2n - \rho$, then

$$\|C^{-1}\| \leq (1 + \gamma \nu_{n,r+\rho-n}^2 \|C_-^{-1}\|) \|C_-^{-1}\|, \text{ for } \gamma \leq \nu_{r+\rho-n}^+ \nu_{r+\rho-n,r+\rho-n}^+ \|C\|, \quad (5.10)$$

for an auxiliary matrix C_- such that the bounds of Corollaries 5.1 and 5.3 on the norm $\|C^{-1}\|$ apply to the norm $\|C_-^{-1}\|$ as well.

Proof. In the proof we encounter matrices that are nonsingular with probability 1, by virtue of Theorem B.1. Due to Assumption 1, we invert them with no further comments.

At first write $r_- = n - \rho$, fix $r_+ \geq r_-$, let

$$r = r_+ + n \geq 2n - \rho,$$

and partition the matrices U and V as follows,

$$U = (U_+ \mid U_n) \text{ and } V = (V_+ \mid V_n)$$

where

$$U_+, V_+ \in \mathcal{G}^{n \times r_+} \text{ and } U_n, V_n \in \mathcal{G}^{n \times n}.$$

Note that

$$C = C_+ + U_n V_n^T = U_n (U_n^{-1} C_+ + V_n^T) \text{ for } C_+ = A + U_+ V_+^T.$$

³Hereafter we use the acronym *SMW*.

Hence

$$C^{-1} = (U_n^{-1}C_+ + V_n^T)^{-1}U_n^{-1} \text{ and } \|C^{-1}\| \leq \|(U_n^{-1}C_+ + V_n^T)^{-1}\| \|U_n^{-1}\|.$$

Recall that $\|(U_n^{-1}C_+ + V_n^T)^{-1}\| = \nu_n^+$ and $\|U_n^{-1}\| = \nu_{n,n}^+$, and obtain bound (5.9).

Next we prove bound (5.10). Assume that

$$r_- \leq r < r_- + n = 2n - \rho,$$

and partition the matrices U and V as follows,

$$U = (U_- \mid \bar{U}) \text{ and } V = (V_- \mid \bar{V})$$

where

$$U_-, V_- \in \mathcal{G}^{n \times r_-} \text{ and } \bar{U}, \bar{V} \in \mathcal{G}^{n \times (r-r_-)}.$$

Furthermore, write $C_- = A + U_- V_-^T$ and $C = C_- + \bar{U} \bar{V}^T$ and, by applying Gaussian diagonalization, reduce our study to the case where C_- is the $n \times n$ diagonal matrix of its singular values, $C_- = \Sigma_{C_-}$.

Represent the matrix C^{-1} by applying the SMW formula (5.8), write

$$S_{r-r_-} = I_{r-r_-} + \bar{V}^T \Sigma_{C_-}^{-1} \bar{U} \text{ and } \gamma = \|(S_{r-r_-}^{-1})\|,$$

recall that $\|\bar{U}\| = \nu_{n,r-r_-}$ and $\|\bar{V}\| = \nu_{n,r-r_-}$, and obtain

$$\|C^{-1}\| \leq (1 + \|\bar{U}\| \gamma \|\bar{V}\| \|C_-^{-1}\|) \|C_-^{-1}\| = (1 + \gamma \nu_{n,r-r_-}^2 \|C_-^{-1}\|) \|C_-^{-1}\|$$

where the upper bounds of Corollaries 5.1 and 5.3 hold for $\|C^{-1}\|$ replaced by $\|C_-^{-1}\|$.

It remains to estimate γ . Partition the matrices \bar{U} , \bar{V} , and Σ_{C_-} as follows,

$$\bar{V}^T = (\bar{V}_{r-r_-}^T \mid \bar{V}_{n-r+r_-}^T), \quad \bar{U}^T = (\bar{U}_{r-r_-}^T \mid \bar{U}_{n-r+r_-}^T), \text{ and } \Sigma_{C_-} = \text{diag}(\Sigma_{C_-,r-r_-}, \Sigma_{C_-,n-r+r_-})$$

where

$$\bar{U}_k^T, \bar{V}_k^T \in \mathcal{G}^{(n-r+r_-) \times k} \text{ and } \Sigma_{C_-,k} \in \mathbb{R}^{k \times k}, \text{ for } k = r-r_-, n-r+r_-.$$

Write $B = I_{r-r_-} + \bar{V}_{n-r+r_-}^T \Sigma_{C_-,n-r+r_-}^{-1} \bar{U}_{n-r+r_-}$ and $\bar{B} = \Sigma_{C_-,r-r_-} \bar{V}_{r-r_-}^{-T} B + \bar{U}_{r-r_-}$ and note that

$$S = I_{r-r_-} + \bar{V}^T \Sigma_{C_-}^{-1} \bar{U} = B + \bar{V}_{r-r_-}^T \Sigma_{C_-,r-r_-}^{-1} \bar{U}_{r-r_-} = \bar{V}_{r-r_-}^T \Sigma_{C_-,r-r_-}^{-1} \bar{B},$$

and so

$$S^{-1} = \bar{B}^{-1} \Sigma_{C_-,r-r_-} \bar{V}_{r-r_-}^{-T} \text{ and } \gamma = \|S^{-1}\| \leq \|\bar{B}^{-1}\| \|\Sigma_{C_-,r-r_-}\| \|\bar{V}_{r-r_-}^{-T}\|.$$

Note that

$$\|\bar{V}_{r-r_-}^{-T}\| = \nu_{r-r_-,r-r_-}^+, \quad \|\Sigma_{C_-,r-r_-}\| = \|C\|, \text{ and } \|\bar{B}^{-1}\| = \nu_{r-r_-}^+,$$

and so

$$\gamma \leq \nu_{r-r_-,r-r_-}^+ \nu_{r-r_-}^+ \|C\|.$$

This completes our proof of bound (5.10). \square

Next we extend Theorem 5.4 to the case where $m \neq n$. With no loss of generality we let $m \geq n$.

Theorem 5.5. *Assume that A is an $m \times n$ matrix such that $\|A\| = 1$, $\text{nrang}(A) = \rho \geq n - r$, $m \geq n > \rho$, $U \in \mathcal{G}^{m \times r}$, $V \in \mathcal{G}^{n \times r}$, and $C = A + UV^T$.*

Then

$$\|C\| \leq \|A\| + \|U\| \|V\| \leq \|A\| + \nu_{m,r} \nu_{n,r}, \quad (5.11)$$

the matrix C has full rank (with probability 1), and bounds of Theorem 5.4 apply to the norm $\|C^+\|$ replacing the norm $\|C^{-1}\|$.

Proof. We only estimate the norm $\|C^+\|$.

By applying Gaussian diagonalization reduce the problem to the case where the matrix A is replaced by the diagonal matrix Σ_A of its singular values.

Pre-multiply the equation $C = A + UV^T$ by the matrix $I_{n,m} = (I_n \mid O_{n,m-n})$, write $C_n = I_{n,m}C$, $\Sigma_{A,n} = I_{n,m}\Sigma_A$, and $U_n = I_{n,m}U$, and obtain that $C_n = \Sigma_{A,n} + U_nV^T$, $\sigma_j(C) \geq \sigma_j(C_n)$ for all j , and so $\|C^+\| \leq \|C_n^{-1}\|$. Apply Theorem 5.4 to the matrices $\Sigma_{A,n}$, U_n , and C_n replacing the matrices A , U , and C , respectively. \square

6 Can We Weaken Randomness?

6.1 Structured and sparse randomization: missing formal support for its empirical power

Would the results of the previous two sections still hold if we weaken randomness of the matrices U , V and W by choosing them sparse, structured, or defined under other probability distributions rather than Gaussian? For the goal of producing matrices of full rank (with probability 1), the answer is “yes” (cf. [BP94, Section 2.13], [PZ15], [PZa], and [PZb]), but would the pre-processed matrices be also well-conditioned?

The affirmative answer is known for low-rank approximation by means of random oversampling, but only for a narrow class of structured preprocessing, and such results have only been proven at the price of allowing a much greater probability of failure versus Gaussian preprocessing. These results can be readily extended to augmentation and additive preprocessing (see the next subsection).

In our tests we have observed consistently that replacing Gaussian preprocessors by sparse and structured preprocessors of a much wider class neither weakens the efficiency of our preprocessing nor increases the frequency of its failure. In Sections 6.3–6.5 we formally support these observations, by applying our techniques of duality and derandomization.

6.2 Structured randomization with SRFT and subcirculant matrices

Preprocessing with SRFT structured matrices (cf. Appendix C) is efficient for low-rank approximation of a matrix by means of random oversampling (cf. [HMT11, Section 11]). By using Theorem C.1 and Remark C.1, we readily extend this property to the case of randomized augmentation and additive preprocessing. Namely, as in the case of low-rank approximation, SRFT preprocessing still works efficiently for the worst case input with a probability close to 1, although this is proven only for SRFT matrices of larger size (due to using the oversampling parameter $\rho_+ - \rho$ in Theorem C.1 and Remark C.1) and at the price of accepting a greater probability of failure compared to the case of Gaussian preprocessing (see Remark C.2). [HMT11, Section 4.6] lists a few other classes of structured matrices as alternatives that have power similar to the SRFT matrices.

In the case of western augmentation with SRFT, our analysis boils down to bounding the norms $\|U_{00}\|$ and $\|\bar{U}^+\|$ where the matrices U_{00} and \bar{U} are the blocks of the matrix $S_A^T U = \begin{pmatrix} U_0 \\ U_1 \end{pmatrix}$, S_A is the orthogonal matrix of the left singular vectors of the $m \times n$ input matrix A , and U is an $n \times q$ SRFT matrix, for q satisfying

$$4\left(\sqrt{m-\rho} + \sqrt{8(m-\rho)m}\right)^2 \log(m-\rho) \leq q \leq m.$$

It remains to analyze randomized western augmentation based on Theorem C.1, which implies that the probability of failure is $O(\frac{1}{m-\rho})$ in our case. If $m-\rho \gg \log(m)$, then we can obtain a little more favorable lower estimates for q , based on Remark C.1.

The result is readily extended to the case of northern and then northwestern augmentation with SRFT. Similarly we can extend our analysis of additive preprocessing based on Theorem C.1 and Remark C.1. We omit the details.

Fact D.1 implies that Theorem C.1 and Remark C.1 still hold if we replace an $n \times \rho_+$ SRFT matrix by the matrix $\frac{n}{l_+} CR$, that is, by the scaled product of an $n \times n$ random circulant matrix

$Z = (z_{i-j \bmod n})_{i,j=0}^{n-1}$ and an $n \times \rho_+$ random matrix R of Theorem C.1. If we further substitute the matrices $(I_{\rho_+} \mid O_{n,\rho})^T$ or $(\mid O_{n,\rho} \mid I_{\rho_+})^T$ for the factor R of the SRFT, then instead of SRFT matrices we arrive at subcirculant matrices (defined in Appendix D). If the input matrix A is subcirculant or, more generally, has structure of Toeplitz type (cf. [P01] on these matrices), then using subcirculant preprocessing is attractive because this preserves matrix structure. We cannot extend the proofs of Theorem C.1 and Remark C.1 from SRFT matrices to such blocks, but in our extensive tests the impact of our preprocessing on the condition numbers of the input matrices remained about the same when we properly scaled these blocks and used them instead of SRFT or Gaussian matrices. In the next subsections we provide some formal support for these empirical observations.

6.3 Dual additive preprocessing

According to our study, Gaussian and SRFT augmentation and additive preprocessing are *universal*, that is, produce well-conditioned matrices of full rank with a probability close to 1 *for any* $m \times n$ *input matrix* having numerical rank $\rho < \min\{m, n\}$.

Next we observe (cf. Section 1) that additive preprocessing with any well-conditioned matrix of full rank applied to *average input matrix* defined under the Gaussian probability distribution is as efficient as Gaussian preprocessing. It follows that preprocessing with a sparse and structured well-conditioned matrix of full rank is efficient when it is applied to a statistically typical input matrix, that is, to almost any matrix with a narrow class of exceptions.

Let us specify our duality argument. Assume that we are given three positive integers m, n and r , where $m \geq n \geq r$, a pair of $n \times r$ matrices $U \in \mathbb{R}^{m \times r}$ and $V \in \mathbb{R}^{n \times r}$, and another pair of matrices $\bar{U} \in \mathbb{R}^{m \times \rho}$ and $\bar{V} \in \mathbb{R}^{n \times \rho}$, for $\rho = n - r$. Then write $A = \bar{U}\bar{V}^T$ and consider additive preprocessing

$$A = \bar{U}\bar{V}^T \rightarrow C = A + UV^T.$$

So far we assumed that U and V were Gaussian matrices, and the matrices \bar{U} and \bar{V} were fixed. In the *dual case* we assume that U and V is any pair of well-conditioned matrices of full rank r and that the matrices \bar{U} and \bar{V} are Gaussian; then we call the matrix $A = \bar{U}\bar{V}^T$ *factor Gaussian of rank* ρ . Furthermore we call a matrix $\tilde{A} = A + E$ a *small-norm perturbation of a factor Gaussian matrix of rank* ρ if the norm $\|E\|$ is small in context.

Clearly, our analysis in the previous section can be immediately extended to the case where additive preprocessing is applied to a small-norm perturbation \tilde{A} of average factor Gaussian matrix $\bar{U}\bar{V}^T$ having rank ρ ,

$$\tilde{A} = \bar{U}\bar{V}^T + E \rightarrow \tilde{C} = \tilde{A} + UV^T, \quad (6.1)$$

for matrices \bar{U} , \bar{V}^T , and E specified above and for any fixed pair of $n \times r$ well-conditioned normalized matrices U and V of full rank r . Here we assume that average matrix \tilde{A} is defined over all pairs of Gaussian matrices \bar{U} and \bar{V} , which may depend on one another and may even coincide with one another. This result promises *significant simplification of additive preprocessing* by means of enforcing desired structure and patterns of sparseness onto the matrices U and V and should motivate substantial research effort in this direction.

6.4 Dual western augmentation

Next we extend our duality results to western augmentation $A \rightarrow K = (U \mid A)$. So far we studied the case where A was a fixed $m \times n$ matrix having numerical rank ρ and $U \in \mathcal{G}^{m \times q}$, but our next theorem (cf. also Remark 6.1) enables us to extend our analysis to the map

$$\tilde{A} = \bar{U}\bar{V}^T + E \rightarrow \tilde{K} = (U \mid \tilde{A}) \quad (6.2)$$

where \tilde{A} is the same matrix of (6.1), that is, a small-norm perturbation of a factor Gaussian matrix, and U is any normalized well-conditioned matrix of full rank.

Theorem 6.1. Assume that an $m \times q$ matrix U is normalized and has full numerical rank $l = \min\{m, q\}$. Define its randomized western augmentation by the map $A \implies K = (U \mid A)$ for $A = \bar{U}\bar{V}^T$, $\bar{U} \in \mathcal{G}^{m \times \rho}$, and $\bar{V} \in \mathcal{G}^{n \times \rho}$. Then

$$\|K\| \leq \|A\| + \|U\| = 1 + \nu_{m,\rho}\nu_{\rho,n}, \quad (6.3)$$

for the random variables $\nu_{m,\rho}$ and $\nu_{\rho,n}$ of Definition 2.1. Furthermore

- (i) the matrix K is rank deficient or ill-conditioned if $q + \rho < m$.
- (ii) Otherwise it has full rank and
- (iii) satisfies the following bounds,

$$\|K^+\| \leq \|U^+\| \text{ if } q \geq m, \quad (6.4)$$

$$\|K^+\| \leq \|U^+\| \max\{1, \nu_{m-q,\rho}^+ \nu_{\rho,n}^+\} (1 + \nu_{q,\rho} \nu_{q,n}) \text{ if } m - \rho \leq q < m. \quad (6.5)$$

Remark 6.1. By using Theorem A.2 one can extend Theorem 6.1 (and similarly Theorem 6.2) to the case where $\tilde{A} = \bar{U}\bar{V}^T + E$ for a perturbation matrix E of small norm replaces matrix $A = \bar{U}\bar{V}^T$.

Proof. Readily verify bounds (6.3) and (6.4) and part (i). Deduce part (ii) from Theorem B.1.

It remains to prove bound (6.5) provided that $m \leq q + \rho$.

By applying Gaussian diagonalization, reduce this task to the case where the matrix U is the diagonal matrix Σ_U of its singular values, that is,

$$K = \begin{pmatrix} \Sigma_U & G_{q,\rho} G_{\rho,n} \\ O_{m-q,q} & G_{m-q,\rho} G_{\rho,n} \end{pmatrix}$$

where $G_{i,j} \in \mathcal{G}^{i \times j}$, for $i = q$ and $i = m - q$ and for $j = \rho$ and $j = n$.

Write $F = G_{m-q,\rho} G_{\rho,n}$ and let $F = S_F \Sigma_F T_F^T$ be SVD.

Here S_F and Σ_F are $(m - q) \times (m - q)$ matrices (cf. Theorem B.1 and Assumption 1) because $\rho \geq m - q$ by assumption, and $T_F^T \in \mathbb{R}^{(m-q) \times n}$.

Define the map $\bar{K} \rightarrow \hat{K} = \text{diag}(I_q, S_F^T) \bar{K} \text{diag}(I_q, T_F) = \begin{pmatrix} \Sigma_U & G_{q,\rho} G_{\rho,n} \\ O_{m-q,q} & \Sigma_F \end{pmatrix}$ and note that the matrix \hat{K} is nonsingular and that

$$\|K^+\| \leq \|\hat{K}^{-1}\|$$

because the matrices $\text{diag}(I_q, S_F^T)$ and $\text{diag}(I_q, T_F)$ are orthogonal and because $n \geq \rho \geq m - q$.

Deduce readily that

$$\|\hat{K}^{-1}\| \leq (1 + \|G_{q,\rho} G_{\rho,m-q}\|) \max\{1, \|\Sigma_U^{-1}\|\} \max\{1, \|\Sigma_F^{-1}\|\}.$$

Recall that $\|U^+\| = \|\Sigma_U^{-1}\| \geq 1$ because $\|U\| = 1$ and that $\|G_{q,\rho} G_{\rho,m-q}\| \leq \nu_{q,\rho} \nu_{\rho,m-q}$. Hence

$$\|K^+\| \leq \|\hat{K}^{-1}\| \leq (1 + \nu_{q,\rho} \nu_{\rho,m-q}) \|U^+\| \max\{1, \|\Sigma_F^{-1}\|\}.$$

Obtain bound (6.5) by combining this inequality with the estimate $\|\Sigma_F^{-1}\| \leq \nu_{m-q,\rho}^+ \nu_{m-q,n}^+$.

In order to prove the latter estimate, write SVDs $G_{m-q,\rho} = S \Sigma T^T$ and $G_{\rho,n} = \bar{S} \bar{\Sigma} \bar{T}^T$ and observe that $S, \Sigma, \bar{S}, \bar{\Sigma} \in \mathbb{R}^{(m-q) \times (m-q)}$ because $\rho \geq m - q$.

Write $F_- = \Sigma T^T \bar{S} \bar{\Sigma}$ and let $F_- = S_{F_-} \Sigma_{F_-} T_{F_-}^T$ be SVD. Then $S_{F_-}, \Sigma_{F_-}, T_{F_-}^T \in \mathbb{R}^{(m-q) \times (m-q)}$, and so SS_{F_-} and $T_{F_-}^T T^T$ are orthogonal matrices.

Hence we can write $S_F = SS_{F_-}$, $\Sigma_F = \Sigma_{F_-}$, and $T_F^T = T_{F_-}^T T^T$, defining SVD $F = S_F \Sigma_F T_F^T$.

Therefore $\Sigma_F = \Sigma_{F_-}$, $\Sigma_F^{-1} = \Sigma_{F_-}^{-1}$, and so $\|\Sigma_F^{-1}\| = \|\Sigma_{F_-}^{-1}\| \leq \|\Sigma^+\| \|\bar{\Sigma}^+\|$.

Substitute $\|\Sigma^+\| = \|G_{m-q,\rho}^+\| = \nu_{m-q,\rho}^+$ and $\|\bar{\Sigma}^+\| = \|G_{\rho,n}^+\| = \nu_{\rho,n}^+$ and obtain the claimed estimate for Σ_F^{-1} . This completes the proof of bound (6.5) and of the theorem. \square

Next we combine Theorems 6.1, B.2, and B.3 and obtain the following upper bounds on the expected values of the norms $\|K\|$ and $\|K^+\|$ (excluding the case where $q + \rho = m$ and the auxiliary random variable $\nu_{m-\rho,q}^+$ has no expected value).

Corollary 6.1. *Under the assumptions of Theorem 6.1, it holds that*

$$\mathbb{E}(\|K\|) < 1 + (1 + \sqrt{m} + \sqrt{\rho})(1 + \sqrt{n} + \sqrt{\rho}),$$

$$\mathbb{E}(\|K^+\|) \leq \mathbb{E}(\|U^+\|) \text{ if } q \geq m,$$

and if $\rho < n$ and $m - \rho < q < m$, then

$$\mathbb{E}(\|K^+\|) < (1 + (1 + \sqrt{\rho} + \sqrt{q})(1 + \sqrt{n} + \sqrt{q})) \max\{1, \frac{(m-q)\rho e^2}{(\rho+q-m)(n-\rho)}\}, \quad e = 2.71828 \dots$$

Remark 6.2. *Theorem 6.1 shows that dual western augmentation is likely to produce a well-conditioned matrix K , particularly where the matrix U is well-conditioned, the integers m and n are not large, and the ratio $\frac{(m-q)\rho}{(\rho+q-m)(n-\rho)}$ is small. We can partly control this ratio by choosing the integer parameter q , and we can readily choose a well-conditioned or even orthogonal matrix U .*

By applying the theorem to the matrix A^T , we can extend it to northern augmentation, that is, to appending a Gaussian block of $s \geq n - \rho$ rows on the top of the matrix A .

6.5 Dual northwestern augmentation

Our next subject is northwestern augmentation given by the map

$$A \rightarrow K = \begin{pmatrix} O_{s,q} & V^T \\ U & A \end{pmatrix}, \quad (6.6)$$

which is the map (6.6) for $W = O_{s,q}$.

Theorem 6.2. *(Cf. Remarks 6.1 and 6.3.) Assume that $U \in \mathbb{R}^{m \times q}$, $V \in \mathbb{R}^{n \times s}$, $\|U\| = \|V\| = 1$, the matrices U and V have full rank, $A = \bar{U}\bar{V}^T$, $\bar{U} \in \mathcal{G}^{m \times \rho}$, $\bar{V} \in \mathcal{G}^{n \times \rho}$, and K is a matrix of (6.6).*

(i) *Then $\|K\| \leq \|U\| + \|V\| + \nu_{m,\rho}\nu_{\rho,n}$.*

(ii) *If $q + \rho < m$ and $s + \rho < n$, then the matrix K is rank deficient. Otherwise it has full rank.*

(iii) *If $q \geq m$ or $s \geq n$, then $\|K^+\| \leq \|U^+\| \|V^+\| (1 + \nu_{m,\rho}\nu_{\rho,n})$.*

(iv) *If $m - \rho \leq q \leq m$ or $n - \rho \leq s \leq n$, then there is an auxiliary nonsingular $(\rho + q + s) \times (\rho + q + s)$ matrix \bar{K} such that*

$$\|K^+\| \leq \|U^+\| \max\{\|V^+\|, \nu_{m-q,\rho}^+ \nu_{\rho,n-s}^+\} \|\bar{K}^{-1}\| \quad (6.7)$$

and

$$\|\bar{K}^{-1}\| \leq 1 + \nu_{l,\rho} \max\{\nu_{q,\rho}, \nu_{m-q,\rho}^+ \nu_{\rho,n-s}^+ \nu_{\rho,s}\} + \nu_{q,\rho} \nu_{\rho,s} (1 + \nu_{\rho,l}^2) \nu_{m-q,\rho}^+ \nu_{\rho,n-s}^+, \quad (6.8)$$

for $l = \min\{m - q, n - s\}$.

Proof. We will only prove part (iv). By applying Gaussian diagonalization, reduce the task to the case where the matrices U and V are replaced by the diagonal matrices of their singular values. Consequently we arrive at the matrix

$$\begin{pmatrix} O_{s,q} & \Sigma_{V^T} & O_{s,n-s} \\ \Sigma_U & G_{q,\rho} G_{\rho,s} & G_{q,\rho} G_{\rho,n-s} \\ O_{m-q,q} & G_{m-q,\rho} G_{\rho,s} & G_{m-q,\rho} G_{\rho,n-s} \end{pmatrix}$$

where $G_{i,j} \in \mathcal{G}^{i \times j}$ for $i = q, \rho, m - q$ and $j = s, \rho, n - s$.

By performing row and column interchange we successively arrive at the matrices

$$\begin{pmatrix} \Sigma_{V^T} & O_{s,q} & O_{s,n-s} \\ G_{q,\rho} G_{\rho,s} & \Sigma_U & G_{q,\rho} G_{\rho,n-s} \\ G_{m-q,\rho} G_{\rho,s} & O_{m-q,q} & G_{m-q,\rho} G_{\rho,n-s} \end{pmatrix}, \quad \begin{pmatrix} \Sigma_{V^T} & O_{s,n-s} & O_{s,q} \\ G_{q,\rho} G_{\rho,s} & G_{q,\rho} G_{\rho,n-s} & \Sigma_U \\ G_{m-q,\rho} G_{\rho,s} & G_{m-q,\rho} G_{\rho,n-s} & O_{m-q,q} \end{pmatrix},$$

and

$$\hat{K} = \begin{pmatrix} \Sigma_{V^T} & O_{s,n-s} & O_{s,q} \\ G_{m-q,\rho}G_{\rho,s} & G_{m-q,\rho}G_{\rho,n-s} & O_{m-q,q} \\ G_{q,\rho}G_{\rho,s} & G_{q,\rho}G_{\rho,n-s} & \Sigma_U \end{pmatrix}.$$

Note that $\sigma_j(\hat{K}) = \sigma_j(K)$, for all j , and thus $\|K^+\| = \|\hat{K}^+\|$.

Write $F = G_{m-q,\rho}G_{\rho,n-s}$ and let $F = S_F \Sigma_F T_F^T$ be SVD.

For $l = \min\{m-q, n-s\}$, write $\Sigma_{l,F} = \text{diag}(\sigma_j(F))_{j=1}^l$ and either $\Sigma_F = (\Sigma_{l,F} \mid O_{l,n-s-l})$ if $m-q \leq n-s$ or $\Sigma_F^T = (\Sigma_{l,F} \mid O_{l-n+s,n-1}^T)$ if $m-q \geq n-s = l$.

By deleting $n-s-m+q$ columns of the matrices F and \hat{K} if $m-q \leq n-s$ or their $m-q-n+s$ rows if $m-q \geq n-s$, we obtain nonsingular matrices \bar{F} and

$$K' = \begin{pmatrix} \Sigma_{V^T} & O_{s,l} & O_{s,q} \\ G_{l,\rho}G_{\rho,s} & \bar{F} & O_{l,q} \\ G_{q,\rho}G_{\rho,s} & G_{q,\rho}G_{\rho,l} & \Sigma_U \end{pmatrix},$$

with SVD $\bar{F} = S_{\bar{F}} \Sigma_{\bar{F}} T_{\bar{F}}^T$, where $S_{\bar{F}}, \Sigma_{\bar{F}} = \Sigma_F, T_{\bar{F}}^T, \bar{F} \in \mathbb{R}^{l \times l}$ and $\|K^+\| = \|\hat{K}^+\| \leq \|(K')^{-1}\|$ by virtue of Lemma A.3.

Note that

$$K' = \text{diag}(\Sigma_{V^T}, \bar{F}, I_q) \bar{K} \text{diag}(I_{l+s}, \Sigma_U),$$

for

$$\bar{K} = \begin{pmatrix} I_s & O_{s,l} & O_{s,q} \\ \bar{F}^{-1}G_{l,\rho}G_{\rho,s} & I_l & O_{l,q} \\ G_{q,\rho}G_{\rho,s} & G_{q,\rho}G_{\rho,l} & I_q \end{pmatrix} = I_{l+q+s} + \begin{pmatrix} O_{s,s} & O_{s,l} & O_{s,q} \\ \bar{F}^{-1}G_{l,\rho}G_{\rho,s} & O_{l,l} & O_{l,q} \\ G_{q,\rho}G_{\rho,s} & G_{q,\rho}G_{\rho,l} & O_{q,q} \end{pmatrix}.$$

Hence $(K')^{-1} = \text{diag}(I_{l+s}, \Sigma_U^{-1}) \bar{K}^{-1} \text{diag}(\Sigma_{V^T}^{-1}, \bar{F}^{-1}, I_q)$ where

$$\bar{K}^{-1} = \begin{pmatrix} I_s & O_{s,l} & O_{s,q} \\ -\bar{F}^{-1}G_{l,\rho}G_{\rho,s} & I_l & O_{l,q} \\ H & -G_{q,\rho}G_{\rho,l} & I_q \end{pmatrix} = I_{l+q+s} - \begin{pmatrix} O_{s,s} & O_{s,l} & O_{s,q} \\ \bar{F}^{-1}G_{l,\rho}G_{\rho,s} & O_{l,l} & O_{l,q} \\ H & G_{q,\rho}G_{\rho,l} & O_{q,q} \end{pmatrix}$$

and

$$H = G_{q,\rho}G_{\rho,l}\bar{F}^{-1}G_{l,\rho}G_{\rho,s} - G_{q,\rho}G_{\rho,s}.$$

Therefore

$$\|K^+\| \leq \max\{1, \|\Sigma_U^{-1}\|\} \|\bar{K}^{-1}\| \max\{1, \|\Sigma_{V^T}^{-1}\|, \|\bar{F}^{-1}\|\},$$

and so

$$\|K^+\| \leq \|U^+\| \|\bar{K}^{-1}\| \max\{\|V^+\|, \|\bar{F}^{-1}\|\}$$

because $\|\Sigma_U^{-1}\| = \|U^+\| \geq 1$ and $\|\Sigma_{V^T}^{-1}\| = \|V^+\| \geq 1$ since $\|U\| = \|V\| = 1$.

Substitute

$$\|\bar{K}^{-1}\| \leq 1 + \|G_{l,\rho}\| \max\{\|F^{-1}\| \|G_{\rho,s}\|, \|G_{q,\rho}\|\} + \|H\| = 1 + \nu_{l,\rho} \max\{\|F^{-1}\| \nu_{\rho,s}, \nu_{q,\rho}\} + \|H\|,$$

$$\|H\| \leq \|G_{q,\rho}\| \|G_{\rho,s}\| (1 + \|G_{\rho,l}\|^2 \|\bar{F}^{-1}\|) \leq \nu_{q,\rho} \nu_{\rho,s} (1 + \nu_{\rho,l}^2 \|\bar{F}^{-1}\|),$$

and

$$\|\bar{F}^{-1}\| \leq \|F^+\| \leq \|G_{m-q,\rho}^+\| \|G_{\rho,n-s}^+\| = \nu_{m-q,\rho}^+ \nu_{\rho,n-s}^+.$$

By combining the above bounds obtain part (iv) of the theorem. \square

Combine Theorems 6.2, B.2, and B.3, exclude the case where $q + \rho = m$ or $s + \rho = n$, in which the auxiliary random variable $\nu_{m-\rho,q}^+$ or $\nu_{n-\rho,s}^+$ has no expected value, and obtain the following bounds.

Corollary 6.2. *It holds that*

$$\mathbb{E}(\|K\|) < 2 + (1 + \sqrt{m} + \sqrt{\rho})(1 + \sqrt{n} + \sqrt{\rho})$$

under the assumptions of part (i) of Theorem 6.1,

$$\mathbb{E}(\|K^+\|) \leq \mathbb{E}(\|U^+\|) \mathbb{E}(\|V^+\|)(1 + (1 + \sqrt{\rho} + \sqrt{m})(1 + \sqrt{\rho} + \sqrt{n}))$$

under the assumptions of its part (iii), and

$$\mathbb{E}(\|K^+\|) \leq \mathbb{E}(\|U^+\|) \max\{\mathbb{E}(\|V^+\|), \mathbb{E}(\|F^+\|)\} \mathbb{E}(\|\bar{K}^{-1}\|),$$

under the assumptions of part (iv) of Theorem 6.1 provided that

$$\mathbb{E}(\|F^+\|) \leq \frac{\sqrt{(m-q)\rho}}{|q + \rho - m| |s + \rho - n|},$$

$$\begin{aligned} \mathbb{E}(\|\bar{K}^{-1}\|) &\leq 1 + (1 + \sqrt{l} + \sqrt{\rho}) \max\{(1 + \sqrt{\rho} + \sqrt{q}), (1 + \sqrt{\rho} + \sqrt{s})\mathbb{E}(\|F^+\|)\} + \\ &\quad (1 + \sqrt{\rho} + \sqrt{q})(1 + \sqrt{\rho} + \sqrt{s})(1 + (1 + \sqrt{\rho} + \sqrt{l})^2)\mathbb{E}(\|F^+\|), \end{aligned}$$

$q + \rho > m$ or $s + \rho > n$, and $(q + \rho - m)(s + \rho - n) \neq 0$.

Remark 6.3. *The upper estimates of Theorem 6.2 and Corollary 6.2 are a little greater than those of Theorem 6.1 and Corollary 6.1, but still show that the dual northwestern augmentation is likely to produce a well-conditioned matrix K , particularly where the matrices U and V (of our choice) are well-conditioned, the integers m and n are not large, and the ratio $\frac{\sqrt{(m-q)\rho}}{|q+\rho-m| |s+\rho-n|}$ is small, which we can partly control by choosing the integer parameters q and s .*

6.6 Some policies of derandomization

The main advantage of dual augmentation and additive preprocessing is a chance for simplifying the computations by means of choosing sparse and structured auxiliary matrices U and V . The matrices U and V of Section 7.2 can be examples: they are extremely sparse, very much structured, orthogonal up to scaling, and have supported efficient preprocessing in our extensive tests. Further examples of simple but empirically highly efficient preprocessors can be found in [PZa] and [PZb].

Here is a caveat, however. Consider western augmentation (6.2) with a fixed sparse and structured preprocessor U having full numerical rank ρ_+ . Although its application is proven to be efficient for average $m \times n$ matrix \tilde{A} having numerical rank $\rho \leq \rho_+$, it may fail for most or all such matrices \tilde{A} from a selected input class. Similar problems can occur for northwestern augmentation and additive preprocessing.

We are likely to exclude running into such bad inputs if we choose universal preprocessing, e.g., with SRFT matrices. The user and the algorithm designer, however, should weight this benefit versus simplification of the computations with non-universal sparse and structured preprocessors.

The following two sample policies keep preprocessing less restricted than universal preprocessing: they do not exclude but just narrow the chances for running into bad inputs.

(i) To any fixed input matrix, apply augmentation or additive preprocessing successively or concurrently, for a small number of distinct preprocessors, pairs of preprocessors, or policies of preprocessing, assuming that the user accepts the output of even a single successful application.

(ii) Alternatively choose a preprocessor or a pair of preprocessors at random from a fixed class of sparse or structured matrices. Empirically this approach consistently produces desired outputs for a variety of inputs (see Table 7.4). This should encourage choosing preprocessors at random from the classes of matrices defined by a small number of real or complex random parameters, or even just by the signs \pm of some integer parameters, as in the tests reported in Table 7.4.

PART III: Numerical Tests, Summary, and Extensions

7 Numerical Experiments

Our numerical experiments have been performed in the Graduate Center of the City University of New York on a Dell server with a dual core 1.86 GHz Xeon processor and 2G memory running Windows Server 2003 R2. The test of the next subsection have been performed by using Fortran code compiled with the GNU gfortran compiler within the Cygwin environment, and all random numbers have been generated with the random_number intrinsic Fortran function, assuming the standard Gaussian probability distribution. The tests have been performed with MATLAB, using its build-in Gaussian random number generating function "randn()", except for the random choice of signs $-$ and $+$ specified at the end of Section 7.2. We applied no iterative refinement in the tests. Their results are in rather good accordance with the results of our formal analysis.

7.1 Approximation of the leading and trailing singular spaces, computation of numerical ranks, and low-rank approximation of a matrix

Tables 7.1–7.3 show the results of our tests where we approximated the bases for the leading and trailing singular spaces $\mathbb{T}_{\rho,A}$ and $\mathbb{T}_{A,\rho}$ of an $n \times n$ matrix A , respectively. The matrix had numerical rank ρ and the condition number $\kappa(A) = 10^{10}$.

We performed the tests for various pairs of n and ρ and observed reasonably close approximations, having the error norms in the range from 10^{-6} to 10^{-9} . The results were similar for Gaussian multipliers and Gaussian subcirculant multipliers. The latter multiplier is a leftmost block of an $n \times n$ circulant matrix that contains the entire first column of a circulant matrix filled with n i.i.d. standard Gaussian variables (cf. Appendix D).

Next we describe the tests in some detail.

GENERATION OF THE INPUTS.

We generated every $n \times n$ input matrix A for our tests of this subsection as follows (cf. [H02, Section 28.3]). At first we fixed n nonnegative values $\sigma_1, \dots, \sigma_n$ and the matrix $\Sigma_A = \text{diag}(\sigma_j)_{j=1}^n$, then generated $n \times n$ random orthogonal matrices S_A and T_A (as the Q -factors of Gaussian matrices), and finally multiplied the three matrices together with infinite precision to output the matrix $A = S_A \Sigma_A T_A^T$. We performed all the other computations of this subsection with double precision, and also rounded all Gaussian values to double precision.

Our $n \times n$ matrices A have numerical rank $\rho = n - r$ and numerical nullity $r = n - \rho$ (cf. Appendix A) for $n = 64, 128, 256$, $\rho = 1, 8, 32$. We have chosen $\sigma_j = 1/j$, for $j = 1, \dots, \rho$, and $\sigma_j = 10^{-10}$, for $j = \rho + 1, \dots, n$, which implied that $\|A\| = 1$ and $\kappa(A) = 10^{10}$.

APPROXIMATION OF A BASIS FOR THE TRAILING SINGULAR SPACE DIRECTLY.

At first we applied Algorithms 4.1.1–4.1.3 and then computed the matrix $B_{A,r} Y_{A,r}$ being a least-squares approximation to the matrix $T_{A,r}$. Table 7.1 displays the data from these tests, namely, the average (mean) values of the error norms $\text{rn} = \|B_{A,\rho} Y_{A,\rho} - T_{A,\rho}\|$ and of the standard deviations observed in 1000 runs of our tests for every pair of n and r . *The tests show superior accuracy of the approximations computed based on randomized northern augmentation.* This is in good accordance with the estimates of Theorems 4.1 and B.3. In particular the latter theorem implies that an $m \times n$ Gaussian matrix is likely to become better conditioned as the value $|m - n|$ increases from 1.

In our tests the accuracy of the outputs has not varied much when we replaced Gaussian matrices by Gaussian subcirculant ones (of Appendix D).

APPROXIMATION OF A BASIS FOR THE LEADING SINGULAR SPACE AND LOW-RANK APPROXIMATION OF A MATRIX.

We have also performed similar tests for the approximation of the leading singular spaces $\mathbb{T}_{\rho,A}$ of the same $n \times n$ matrices A , which had numerical rank ρ , and for the approximation of such a matrix A with a matrix of rank ρ . At first we generated $n \times \rho$ Gaussian matrices U and Gaussian subcirculant $n \times \rho$ matrices \bar{U} (in both cases for $\rho = 8$ and $\rho = 32$) and then successively computed the matrices $B_{\rho,A} = A^T U$ and $B_{\rho,A} = A^T \bar{U}$ (in order to obtain approximate matrix bases for the leading singular space $\mathbb{T}_{\rho,A}$), $B_{\rho,A} Y_{\rho,A}$ as a least-squares approximation to $T_{\rho,A}$, $Q_{\rho,A} = Q(B_{\rho,A})$, and $A - A Q_{\rho,A} (Q_{\rho,A})^T$, which is the error matrix of the approximation of the matrix A based on the

Table 7.1: Error norms of the approximation of the trailing singular space directly

n	r	Gaussian Multipliers			Gaussian Subcirculant Multipliers		
		Alg. 3.1.1	Alg 3.1.2	Alg 3.1.3	Alg 3.1.1	Alg 3.1.2	Alg 3.1.3
64	2	7.91e-07	7.91e-07	2.77e-14	1.35e-07	1.35e-07	3.03e-14
64	4	2.46e-07	2.46e-07	4.18e-14	3.26e-07	3.26e-07	4.76e-14
64	8	2.70e-07	2.70e-07	6.48e-14	4.90e-07	4.90e-07	8.93e-14
128	2	4.64e-07	4.64e-07	6.03e-14	8.41e-07	8.41e-07	6.29e-14
128	4	5.33e-07	5.33e-07	1.27e-13	1.01e-06	1.01e-06	1.12e-13
128	8	2.88e-06	2.88e-06	1.79e-13	8.82e-07	8.82e-07	1.81e-13
256	2	2.16e-06	2.16e-06	7.29e-13	1.34e-06	1.34e-06	6.10e-13
256	4	2.07e-06	2.07e-06	2.97e-13	3.38e-06	3.38e-06	4.60e-13
256	8	3.66e-06	3.66e-06	5.86e-13	3.80e-06	3.80e-06	5.06e-13

approximation of a basis for its leading singular space. Table 7.2 displays the data on the average error norms $\text{rn}_1 = \|B_{\rho,A}Y_{\rho,A} - T_{\rho,A}\|$ and $\text{rn}_2 = \|A - AQ_{\rho,A}(Q_{\rho,A})^T\|$ obtained in 1000 runs of our tests for every pair of n and ρ . For our choice of $B_{\rho,A} = A^T U$ and $B_{\rho,A} = A^T \tilde{U}$, the computed error norms were equally small and about as small as in Table 7.1.

Table 7.2: Error norms of the approximation of the leading singular spaces and of low-rank approximation of a matrix

			Gaussian Multipliers		Subcirculant Multipliers	
ρ	rn_i	n	mean	std	mean	std
8	rn_1	64	4.26e-07	8.83e-07	1.43e-07	9.17e-07
8	rn_1	128	4.30e-08	1.45e-07	4.87e-07	4.39e-06
8	rn_1	256	3.40e-08	5.11e-08	6.65e-08	3.12e-07
8	rn_2	64	5.77e-09	1.06e-08	6.37e-08	4.11e-07
8	rn_2	128	1.86e-08	5.97e-08	1.90e-07	1.67e-06
8	rn_2	256	1.59e-08	2.47e-08	2.92e-08	1.28e-07
32	rn_1	64	1.01e-07	3.73e-07	4.06e-08	6.04e-08
32	rn_1	128	1.28e-07	6.76e-07	2.57e-07	8.16e-07
32	rn_1	256	1.02e-07	1.54e-07	1.18e-07	2.03e-07
32	rn_2	64	2.30e-08	8.28e-08	9.66e-09	1.48e-08
32	rn_2	128	2.87e-08	1.45e-07	5.50e-08	1.68e-07
32	rn_2	256	2.37e-08	3.34e-08	2.74e-08	4.48e-08

EXTENSION FROM THE LEADING TO THE TRAILING SINGULAR SPACES.

Finally we approximated the trailing singular spaces $\mathbb{T}_{A,\rho}$ for the same input matrices A as for Table 7.1, where $\rho = n - r$ and $r = 1, 2, 4$, but applied Algorithm 3.1t. At first we applied Algorithm 2.1, which outputs an approximate matrix basis $B_{\rho,A}$ for the leading singular space $\mathbb{T}_{\rho,A}$. Then we applied [PQ12, Algorithm 4.1] in order to compute the matrix $B_{A,\rho} = \text{nmb}(B_{\rho,A})$, being an approximate matrix basis for the trailing singular space $\mathbb{T}_{A,\rho}$. Table 7.3 displays the least-squares error norms $\text{rn} = \|B_{A,\rho}Y_{A,\rho} - T_{A,\rho}\|$. They slightly exceed those of Table 7.1.

7.2 Preconditioning tests

Table 7.4 covers our tests for the preconditioning by means of randomized additive preprocessing and augmentation. The tests show great power of both additive preprocessing and augmentation, even though we limited randomization to choosing the signs $+$ and $-$ for the nonzero entries of some

Table 7.3: Error norms of approximate bases of the trailing singular spaces computed as the nmbs of the bases for the leading singular spaces

r	n	mean	std
1	64	2.13e-07	6.87e-07
1	128	3.12e-07	7.20e-07
1	256	9.41e-07	1.49e-06
2	64	1.74e-07	3.02e-07
2	128	4.79e-07	1.12e-06
2	256	1.33e-07	3.04e-06
4	64	7.49e-07	3.90e-06
4	128	7.18e-07	2.63e-06
4	256	3.37e-06	9.27e-06

very sparse and highly structured matrices U , V , and W . Namely, both our additive preprocessing and augmentation consistently decreased the condition numbers of the input matrices from about 10^{16} to the values in the range from 10^2 to $5 * 10^5$.

GENERATION OF THE INPUTS.

We have tested the input matrices of the following classes.

1n. *Nonsymmetric matrices A of type I with numerical nullity $r = n - \text{nrnk}(A)$.* $A = S\Sigma_r T^T$ are $n \times n$ matrices where S and T are $n \times n$ random orthogonal matrices, that is, the factors Q in the QR factorizations of random real matrices; $\Sigma_r = \text{diag}(\sigma_j)_{j=1}^n$ is the diagonal matrix such that $\sigma_{j+1} \leq \sigma_j$ for $j = 1, \dots, n-1$, $\sigma_1 = 1$, the values $\sigma_2, \dots, \sigma_{n-r-1}$ are randomly sampled in the semi-open interval $[0.1, 1)$, $\sigma_{n-r} = 0.1$, $\sigma_j = 10^{-16}$ for $j = n-r+1, \dots, n$, and therefore $\kappa(A) = 10^{16}$ [H02, Section 28.3].

1s. *Symmetric matrices of type I with numerical nullity r .* The same as in part 1n, but for $S = T$.

The matrices of the six other classes have been constructed in the form of $\frac{A}{\|A\|} + \beta I$, with the recipes for defining the matrices A and scalars β specified below.

2n. *Nonsymmetric matrices of type II with numerical nullity r .* $A = (W \mid WZ)$ where W and Z are random orthogonal matrices of sizes $n \times (n-r)$ and $(n-r) \times r$, respectively.

2s. *Symmetric matrices of type II with numerical nullity r .* $A = WW^T$ where W are random orthogonal matrices of size $n \times (n-r)$.

3n. *Nonsymmetric Toeplitz-like matrices with numerical nullity r .* $A = c(T \mid TS)$ for random Toeplitz matrices T of size $n \times (n-r)$ and S of size $(n-r) \times r$ and for a positive scalar c such that $\|A\| \approx 1$.

3s. *Symmetric Toeplitz-like matrices with numerical nullity r .* $A = cTT^T$ for random Toeplitz matrices T of size $n \times (n-r)$ and a positive scalar c such that $\|A\| \approx 1$.

4n. *Nonsymmetric Toeplitz matrices with numerical nullity 1.* $A = (a_{i,j})_{i,j=1}^n$ is a Toeplitz $n \times n$ matrix. Its entries $a_{i,j} = a_{i-j}$ are random for $i-j < n-1$, and so the matrix $A_{n-1} = (a_{i,j})_{i,j=1}^{n-1}$ is nonsingular (with probability 1) and was indeed nonsingular in all our tests. The entry $a_{n,1}$ is selected to annihilate or nearly annihilate $\det A$, that is, to fulfill

$$\det A = 0 \text{ or } \det A \approx 0, \quad (7.1)$$

in which case the matrix A is singular or ill-conditioned.

4s. *Symmetric Toeplitz matrices with numerical nullity 1.* $A = (a_{i,j})_{i,j=1}^n$ is a Toeplitz $n \times n$ matrix. Its entries $a_{i,j} = a_{i-j}$ are random for $|i-j| < n-1$, while the entry $a_{1,n} = a_{n,1}$ was selected to satisfy equation (7.1), which is the quadratic equation in this entry. Occasionally it had no real roots, but then we repeatedly generated the matrix A .

We set $\beta = 10^{-16}$ for symmetric matrices A in the classes 2s, 3s, and 4s, so that $\kappa(A) = 10^{16} + 1$ in these cases. For nonsymmetric matrices A we defined the scalar β by an iterative process such that $\|A\| \approx 1$ and $10^{-18}\|A\| \leq \kappa(A) \leq 10^{-16}\|A\|$ [PIMR10, Section 8.2].

RANDOMIZED PREPROCESSING AND TEST RESULTS.

Table 7.4 displays the average values of the condition numbers $\kappa(C)$ and $\kappa(K)$ of the matrices $C = A + UV^T$ and $K = \begin{pmatrix} W & V^T \\ U & A \end{pmatrix}$ over 1000 tests for the inputs in the above classes, $r = 1, 2, 4, 8$ and $n = 128$. Here

$$U = \frac{\bar{U}}{\|\bar{U}\|}, \quad \bar{U}^T = (\pm I_r \mid O_{r,r} \mid \pm I_r \mid O_{r,r} \mid \dots \mid O_{r,r} \mid \pm I_r \mid O_{r,s}),$$

s is such that $\bar{U} \in \mathbb{R}^{n \times r}$,

$$V = \frac{\bar{V}}{\|\bar{V}\|}, \quad \bar{V}^T = (2I_r \mid O_{r,r} \mid 2I_r \mid O_{r,r} \mid \dots \mid O_{r,r} \mid 2I_r \mid O_{r,s}) - U^T,$$

$W = \frac{\bar{W}}{\|\bar{W}\|} \in \mathbb{R}^{r \times r}$, \bar{W} are circulant matrices, each defined by its first column, filled with ± 1 , and here as well as in the expression for \bar{U} , all signs \pm turn into $+$ and $-$ with the same probability 0.5, independently of each other.

In our further tests the condition numbers of the matrices $C = A + 10^p UV^T$ for $p = -10, -5, 5, 10$ were steadily growing within a factor $10^{|p|}$ as the value $|p|$ was growing. This showed the importance of proper scaling of the additive preprocessor UV^T .

Table 7.4 also displays the results of the similar tests with Gaussian matrices U , V , and W . The results show similar power of Gaussian preprocessors and our random sparse and structured preprocessors.

Table 7.4: Preconditioning tests

Type	r	$\kappa(C)$, Gaussian	$\kappa(K)$, Gaussian	$\kappa(C)$, structured	$\kappa(K)$, structured
1n	1	1.38e+04	1.80e+04	1.80e+04	2.47e+04
1n	2	9.07e+03	9.66e+03	8.60e+03	2.17e+04
1n	4	6.91e+04	7.14e+04	4.94e+04	2.15e+05
1n	8	2.03e+04	2.20e+04	2.81e+04	1.72e+05
1s	1	4.48e+03	5.76e+03	3.02e+03	1.95e+04
1s	2	2.32e+04	1.95e+04	1.43e+04	8.19e+04
1s	4	2.38e+04	1.89e+04	5.67e+03	7.85e+04
1s	8	7.49e+04	3.32e+04	1.26e+04	1.62e+05
2n	1	6.75e+03	7.38e+03	3.79e+03	4.27e+03
2n	2	1.78e+04	1.75e+04	1.74e+04	3.92e+04
2n	4	3.91e+04	4.44e+04	1.63e+05	1.78e+06
2n	8	4.57e+04	3.00e+04	4.72e+04	4.56e+05
2s	1	1.35e+04	1.72e+04	6.17e+03	1.04e+04
2s	2	1.07e+04	8.81e+03	8.27e+03	3.68e+04
2s	4	2.01e+04	1.23e+04	2.93e+04	1.74e+05
2s	8	2.99e+04	1.77e+04	1.65e+04	2.26e+05
3n	1	4.62e+04	6.49e+04	1.26e+04	2.02e+04
3n	2	2.68e+06	2.98e+06	2.61e+04	5.96e+04
3n	4	4.29e+04	6.28e+04	3.75e+05	1.15e+06
3n	8	1.22e+05	1.79e+05	1.04e+05	4.00e+05
3s	1	5.34e+05	7.67e+05	8.43e+05	1.32e+06
3s	2	2.88e+06	4.07e+06	1.52e+06	3.06e+06
3s	4	1.44e+06	1.99e+06	3.97e+05	1.30e+06
3s	8	9.63e+05	1.32e+06	5.95e+05	2.88e+06
4n	1	4.26e+03	3.67e+03	3.51e+03	3.49e+03
4n	2	6.51e+03	9.84e+03	7.06e+03	5.58e+04
4n	4	4.22e+03	1.45e+04	4.03e+03	1.78e+05
4n	8	4.39e+03	3.40e+04	4.72e+03	3.97e+04
4s	1	4.06e+05	4.14e+05	2.61e+06	2.50e+06
4s	2	1.34e+06	3.79e+04	1.09e+05	3.24e+04
4s	4	1.30e+05	1.51e+04	1.49e+04	4.69e+04
4s	8	2.85e+04	1.17e+04	1.04e+04	6.95e+04

8 Conclusions

We studied randomized preprocessing for the acceleration of computations with singular and ill-conditioned matrices. We assumed that an $m \times n$ input matrix $A - E$ of rank ρ has been represented by its approximation A , with a small perturbation norm $\|E\|$, so that the matrix A had numerical rank ρ . Then we approximated some bases for the range and the null space of the matrix $A - E$, which were the leading and trailing singular spaces $\mathbb{T}_{\rho,A}$ and $\mathbb{T}_{A,\rho}$ of the matrix A , respectively, associated with its ρ largest singular values and its remaining singular values, respectively.

The customary numerical algorithms solve these problems by using pivoting, orthogonalization, or SVD, but by extending our earlier study in [PQ10], [PQ12], and [PQZC] we applied randomization instead of these costly techniques and obtain accurate solution at a significantly lower computational cost. Our null space algorithms reduce the solution of homogeneous rank deficient and ill-conditioned linear systems of equations to the similar tasks for well-conditioned linear systems of full rank, which significantly improves the known algorithms for this fundamental computational problem.

Our work continued the study in a stream of our earlier papers, which empirically demonstrated the preconditioning power of randomized augmentation and additive preprocessing. Now we supplied detailed formal analysis which supported these empirical observations.

In particular our study has shown greater efficiency of western and northern augmentation (that is, appending a block of random rows or columns to the given matrix) versus northwestern augmentation (that is, appending two blocks of random rows or columns simultaneously) and additive preprocessing. This can properly direct randomized preprocessing.

Our formal results have been in good accordance with our previous and present numerical tests, which have consistently shown that great variety of random sparse and structured preprocessors (even where randomization was very limited) usually are as efficient preconditioners as Gaussian ones. Similar observations have been made by ourselves and by many other researchers about the power of random sparse and structured multipliers versus Gaussian multipliers in their applications to low-rank approximation of a matrix and to GENP.

For a long while formal support for these empirical observations has been missing, but our novel duality techniques has provided formal support for these empirical observations.

Our results motivate derandomization of our preprocessing and bolder application of sparse and structured preprocessing for the computational problems studied in this paper as well as for some other important problems of matrix computations. This promises significant acceleration of the known algorithms.

Promising and in some cases surprising findings of this kind have been presented also in [PZa] and [PZb]), and it is a major challenge to find new classes of efficient preprocessors and new areas where our techniques can increase substantially the efficiency of the known algorithms.

In the rest of this section, we outline our novel application of randomized augmentation and additive preprocessing to supporting GENP. The papers [PQZ13], [PQY15], and [PZ15] cover alternative randomized multiplicative support of GENP, its motivation and history.

Suppose that we are given an $n \times n$ matrix A and we try to apply to it GENP and to avoid limitations of multiplicative preprocessing (cf. [PQZ13], [PQY15], and [PZ15]). Fix a positive integer $h < n$ and a pair of $n \times h$ matrices U and V and consider northwestern augmentation and additive preprocessing given by the maps

$$A \rightarrow K = \begin{pmatrix} I_h & V^T \\ U & A \end{pmatrix} \text{ and } C = A - UV^T, \quad (8.1)$$

respectively. Gaussian augmentation and additive preprocessing generate $2hn$ Gaussian parameters each; additive preprocessing requires in addition $(2h - 1)n^2$ flops. By choosing structured (e.g., Toeplitz) matrices U and V , we can decrease these bounds to $O(n)$ random parameters and $O(n \log(n))$ flops.

Theorem 8.1. *Let h and n be two positive integers. Let A be an $n \times n$ matrix normalized so that $\|A\| \approx 1$ and let η denote the maximum numerical nullity of its leading square blocks. Let U and V be the pair of $n \times h$ Gaussian matrices such that either $U = V$ or these two matrices U and V*

are independent of one another. Suppose that equation (8.1) defines northwestern augmentation and additive preprocessing of the matrix A , producing the matrices K and C .

(i) Then these matrices are nonsingular with probability 1, and their condition numbers can be estimated from above according to the probabilistic estimates of Sections 4 and 5.

(ii) One can apply the probabilistic estimates of Section 6 instead if U and V are SRFT matrices, if we choose $h \geq q = cn$, for a sufficiently large constant c , and if

$$4\left(\sqrt{\eta} + \sqrt{8\log_2(\eta n)}\right)^2 \log_2(\eta) \leq h.$$

The claimed results are readily verified for augmentation with Gaussian and SRFT matrices producing matrices K . We extend them to matrices C , produced with additive preprocessing, by applying GENP to the matrix K . Indeed we arrive at the same task for the matrix C in h elimination steps.

In part (i) of Theorem 8.1 we can set $h = \eta$ if we know the bound η , but otherwise we can try to guess such a bound *by actions*. Namely, assume at first that $\eta \leq 1$, set $h = 1$, apply GENP to the matrix K or C , and in the case of failure, increase (e.g., double) h recursively.

Let us motivate this policy. Define the η -family of matrices as the set of all matrices with the maximal numerical nullity at least η for its leading square blocks. Then already the 1-family makes up a small fraction of all matrices, and the size of the η -family decreases very fast as η grows.

This randomized preprocessing is universal and allows us to use SRFT structure, but supports the application of GENP to the matrices K and C , rather than to the original matrix A . Our next goal is the inversion of the matrix A or the solution of a linear system $A\mathbf{x} = \mathbf{b}$ simplified by using the output of the above applications.

A potential tool is the SMW formula (5.8), which we can extend by expressing the inverse A^{-1} through the inverse K^{-1} rather than C^{-1} .

If the assumptions of Theorem 8.1 have been satisfied, then the matrix C is likely to be well-conditioned, but using the SMW formula may still cause numerical problems at the stages of computing and inverting the matrix $I_h + V^T C^{-1} U$.

For a natural antidote, we can perform the computations at these stages with extended precision. They involve $O(hn^2)$ flops, versus the order of n^3 flops involved at the other stages and performed with double precision. This can be attractive when $h \ll n$.

For a large class of well-conditioned matrices A , we can try to avoid numerical problems by scaling the matrices U and V . This is a research challenge, and next we outline some recipes and obstacles.

If the ratio $\frac{\|A\|}{\|UV^T\|}$ is sufficiently large, then $\|VC^{-1}U\| \leq \theta < 1$ for a constant θ not close to 1, and the diagonally dominant matrix $I_h + V^T C^{-1} U$ can be computed and inverted with no numerical problems. The power of that recipe is limited, however, because our randomized preprocessing does not work if the ratio $\frac{\|A\|}{\|UV^T\|}$ is too large.

Application of the homotopy continuation techniques (cf. [P01, Section 6.9], [PKRK06], [P10]) may help to extend the power of this recipe.

For two other policies pointed out below, we must also scale the matrices U and V in order to have a sufficiently large ratio $\frac{\|A\|}{\|UV^T\|}$, and then again this scaling can be in conflict with obtaining our randomized support for GENP for the matrices K , K' , and/or C .

(i) If we achieve scaling such that $\|I - C^{-1}A\| \leq \theta < 1$ for a constant θ not close to 1, then Newton's iteration $X_{i+1} = 2X_i - X_i A X_i$, $i = 0, 1, \dots$, initialized at $X_0 = C^{-1}$, converges quadratically right from the start to the inverse A^{-1} (cf. [P01, Chapter 6]).

(ii) Suppose that we seek the solution of a linear system $A\mathbf{x} = \mathbf{b}$ and that GENP, applied to the matrix $C = A + UV^T$, has output its LU factorization being close to the LU factorization of the matrix A . Then we can solve the linear system $A\mathbf{x} = \mathbf{b}$ accurately by applying iterative refinement.

Appendix

A Some Basic Definitions and Properties of Matrix Computations

A real matrix Q is orthogonal if $Q^T Q = I$ or $Q Q^T = I$.

$\|M\|_F$ is the Frobenius norm of a matrix M .

$A^+ = T_A \text{diag}(\hat{\Sigma}_A^{-1}, O_{n-\rho, m-\rho}) S_A^T$ is the Moore–Penrose pseudo-inverse of the matrix A of (2.1).

$\kappa(A) = \frac{\sigma_1(A)}{\sigma_\rho(A)} = \|A\| \|A^+\|$ is the condition number of an $m \times n$ matrix A of rank ρ . Such matrix is *ill-conditioned* if the ratio $\frac{\sigma_1(A)}{\sigma_\rho(A)} = \|A\| \|A^+\|$ is large and otherwise is *well-conditioned*.

The *numerical rank* of an $m \times n$ matrix A , denoted $\text{nrnk}(A)$, is the minimal rank of its nearby matrices, and $\text{nnul}(A) = n - \text{nrnk}(A)$ is the numerical nullity of A .

Recall the following basic properties.

$$\|A^T\| = \|A\| \leq \|A\|_F = \|A^T\|_F \leq \sqrt{n} \|A\|, \quad \|AB\| \leq \|A\| \|B\|, \quad \|AB\|_F \leq \|A\|_F \|B\|_F, \quad (\text{A.1})$$

$$\|\text{diag}(M_j)_j\| = \max_j \|M_j\| \text{ for any set of matrices } M_j. \quad (\text{A.2})$$

$$\|A^+\| = \frac{1}{\sigma_\rho(A)}. \quad (\text{A.3})$$

Lemma A.1. Suppose $\Sigma = \text{diag}(\sigma_i)_{i=1}^n$, $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_n$, $F \in \mathbb{R}^{r \times n}$, and $H \in \mathbb{R}^{n \times r}$. Then

- $\sigma_j(F\Sigma) \geq \sigma_j(F)\sigma_n$, $\sigma_j(\Sigma H) \geq \sigma_j(H)\sigma_n$ for all j .
- If also $\sigma_n > 0$, then $\text{rank}(F\Sigma) = \text{rank}(F)$ and $\text{rank}(\Sigma H) = \text{rank}(H)$.

Lemma A.2. $\sigma_j(SM) = \sigma_j(MT) = \sigma_j(M)$ for all j if S and T are square orthogonal matrices.

Lemma A.3. For a matrix A , its submatrix A_0 , and a subscript j , it holds that $\sigma_j(A) \geq \sigma_j(A_0)$.

Theorem A.1. We have $|\sigma_j(C) - \sigma_j(C + E)| \leq \|E\|$ for all $m \times n$ matrices C and E and all j .

Proof. See [GL13, Corollary 8.6.2] or [S98, Corollary 4.3.2]. \square

Theorem A.2. Suppose C and $C + E$ are two nonsingular matrices of the same size and $\|C^{-1}E\| = \theta < 1$. Then

- $\|I - (C + E)^{-1}C\| \leq \frac{\theta}{1-\theta}$ and $\|(C + E)^{-1} - C^{-1}\| \leq \frac{\theta}{1-\theta} \|C^{-1}\|$.
- In particular, $\|(C + E)^{-1} - C^{-1}\| \leq 0.5 \|C^{-1}\|$ if $\theta \leq 1/3$.

Proof. See [S98, Corollary 1.4.19] for $P = -C^{-1}E$. \square

Theorem A.3. [S95, Theorem 5.1]. Assume a pair of $m \times n$ matrices A and $A + E$, and let the norm $\|E\|$ be small. Then $\|Q(A + E) - Q(A)\|_F \leq \sqrt{2} \|A^+\| \|E\|_F + O(\|E\|_F^2)$.

B A Gaussian Matrix. Estimates for Its Rank, Norm and Condition Number

Definition B.1. A matrix is said to be standard Gaussian random (hereafter referred to just as Gaussian) if it is filled with i.i.d. Gaussian random variables having mean 0 and variance 1. $\mathcal{G}^{m \times n}$ denotes the class of $m \times n$ Gaussian matrices.

Lemma B.1. Invariance of the products of Gaussian matrices under orthogonal multiplications. Suppose that $H \in \mathbb{R}^{m \times n}$, $S \in \mathbb{R}^{k \times m}$, and $T \in \mathbb{R}^{n \times k}$ for some positive integers k , m , and n , and suppose that the matrices S and T are orthogonal. Then

- (i) $SH \in \mathcal{G}^{k \times n}$ and $HT \in \mathcal{G}^{m \times k}$ if $H \in \mathcal{G}^{m \times n}$ and
- (ii) $SH \in \mathcal{G}_{k,n}$ and $HT \in \mathcal{G}_{m,k}$ if $H \in \mathcal{G}_{m,n}$.

Hereafter we call a vector \mathbf{t} unit if $\|\mathbf{t}\| = 1$.

Lemma B.2. Cf. [SST06, Lemma A.2]. Assume two positive integers n and r , a real μ , a positive x , a unit vector $\mathbf{u} \in \mathbb{R}^{k \times 1}$, and two independent Gaussian vectors $\mathbf{g}_k \in \mathcal{G}^{k \times 1}$ for $k = r$ and $k = r$. Then $\text{Probability}\{|\mathbf{u}^T \mathbf{g}_n - \mu| \leq x\} \leq \sqrt{\frac{2}{\pi}}x$.

Theorem B.1. A Gaussian matrix has full rank with probability 1.

Proof. At first recall that an algebraic variety of a dimension $d \leq N$ in the space \mathbb{R}^N is defined by $N - d$ polynomial equations and cannot be defined by fewer equations. (Fact E.1 specifies the dimension of the algebraic variety of $m \times n$ matrices of rank ρ .) Now assume a rank deficient $m \times n$ matrix where $m \geq n$, say. Then the determinants of all its $n \times n$ submatrices vanish. This implies $\binom{m}{n}$ polynomial equations on the entries, that is, rank deficient matrices form an algebraic variety of a lower dimension in the linear space $\mathbb{R}^{m \times n}$. Clearly, such a variety has Lebesgue (uniform) and Gaussian measures 0, both being absolutely continuous with respect to one another. \square

Theorem B.2. See [DS01, Theorem II.7] and our Definition 2.1.

Suppose that $h = \max\{m, n\}$, $t \geq 0$. Then

- (i) $\text{Probability}\{\nu_{m,n} > t + \sqrt{m} + \sqrt{n}\} \leq \exp(-t^2/2)$, and so
- (ii) $\mathbb{E}(\nu_{m,n}) < 1 + \sqrt{m} + \sqrt{n}$.

Theorem B.3. Suppose that $m \geq n$ and $x > 0$ and let $\Gamma(x) = \int_0^\infty \exp(-t)t^{x-1}dt$ and $\zeta(t) = t^{m-1}m^{m/2}2^{(2-m)/2} \exp(-mt^2/2)/\Gamma(m/2)$ denote the Gamma function. Then

1. $\text{Probability}\{\nu_{m,n}^+ \geq m/x^2\} < \frac{x^{m-n+1}}{\Gamma(m-n+2)}$ for $n \geq 2$,
2. $\text{Probability}\{\nu_{n,n}^+ \geq x\} \leq 2.35\sqrt{n}/x$ for $n \geq 2$ (cf. Remark B.1),
3. $\text{Probability}\{\nu_{m,1}^+ \geq x\} \leq (m/2)^{(m-2)/2}/(\Gamma(m/2)x^m)$ for $m \geq 2$, and
4. $\mathbb{E}((\nu_{F,m,n}^+)^2) = m/|m - n - 1|$ provided that $n > 1$ and $m - n > 1$, while $\mathbb{E}(\nu_{m,n}^+) \leq e\sqrt{l}/|m - n|$ for $e = 2.71828\dots$, $l = \min\{m, n\}$, and $m \neq n$.

Proof. See [CD05, Proof of Lemma 4.1] for part 1 and [HMT11, Proposition 10.2] for part 4. Part 2 follows from (2.3) for $A = O_{n,n}$.

Let us deduce part 3. $G \in \mathbb{R}^{m \times 1}$ is a vector of length m . So, with probability 1 it holds that $G \neq 0$, $\text{rank}(G) = 1$, $\|G^+\| = 1/\|G\|$. Consequently,

$$\text{Probability}\{\|G^+\| \geq x\} = \text{Probability}\{\|G\| \leq 1/x\} \leq \int_0^{1/x} \zeta(t)dt \text{ for } x > 0.$$

Note that $\exp(-mt^2/2) \leq 1$. Hence $\int_0^{1/x} \zeta(t)dt < c_m \int_0^{1/x} t^{m-1}dt = c_m/(mx^m)$ where $\zeta(t) = t^{m-1}m^{m/2}2^{(2-m)/2} \exp(-mt^2/2)/\Gamma(m/2)$ is the Zeta function and $c_m = m^{m/2}2^{(2-m)/2}/\Gamma(m/2)$. \square

Remark B.1. Part 2 of Theorem B.3 provides some bound on the random variable $\nu_{n,n}^+$, although this bound is weaker than the bounds in other parts of the theorem, and the random variable $\nu_{n,n}^+$ has no expected value.

Theorems B.2 and B.3 together imply that the expected value of the condition number of an $m \times n$ Gaussian matrix decreases quite fast as the integer $|m - n|$ increases from 1. This implies greater efficiency of western and northern augmentation versus northwestern one.

Quite tight estimates for the condition numbers $\kappa_{m,n}$ can be found in [D88], [E88], [CD05, Theorem 4.5], and [ES05].

C SRFT Matrices

Next we recall the definition and some basic properties of *SRFT* matrices, by following [HMT11, Section 11.1]. An SRFT is an $n \times \rho$ complex matrix of the form $H = \sqrt{n/\rho_+} D \Omega R$ where

- $D = \text{diag}(d_i)_{i=0}^{n-1}$ is the $n \times n$ is a diagonal matrix, whose diagonal entries d_i are independent and uniformly distributed on the complex unit circle $\{z : |z| = 1\}$;
- Ω is the $n \times n$ unitary matrix of discrete Fourier transform, $\Omega = \frac{1}{\sqrt{n}}(\omega^{ij})_{i,j=0}^{n-1}$ for a primitive root of unity $\omega = \exp(2\pi\sqrt{-1}/n)$; and
- R^T is a random $\rho_+ \times n$ matrix that restricts an n -dimensional vector to ρ_+ coordinates, chosen uniformly at random, for $\rho_+ \geq \rho$.

Up to scaling, an SRFT is just a section of a unitary matrix; it satisfies the norm identity $\|H\| = \sqrt{n/\rho_+}$. The critical fact is that an appropriately designed SRFT approximately preserves the geometry of *an entire subspace of vectors*.

Theorem C.1. The SRFT multiplier is likely to preserve the rank and the condition number. Fix a $\rho \times n$ orthogonal matrix U and generate an $n \times \rho_+$ SRFT matrix H , where the parameter $\rho_+ = \rho_+(\rho, n) \geq \rho$ satisfies

$$4\left(\sqrt{\rho} + \sqrt{8\log(\rho n)}\right)^2 \log(\rho) \leq \rho_+ \leq n.$$

Then

$$0.40 \leq \sigma_\rho(UH) \quad \text{and} \quad \sigma_1(UH) \leq 1.48$$

with the failure probability at most $O(1/\rho)$.

In words, the null space of an $n \times \rho_+$ SRFT matrix with ρ_+ of order $(\rho + \log(n) \log(\rho))$ is unlikely to intersect a fixed ρ -dimensional subspace.

Remark C.1. The logarithmic factor $\log(\rho)$ in the lower bound on ρ_+ can be decreased for larger n (see below), but in contrast with the Gaussian case, cannot generally be removed, that is, with SRFT matrices we involve a positive oversampling integer parameter $\rho_+ - \rho$. For large problems, one can reduce the numerical constants of Theorem C.1. If $\rho \gg \log(n)$ and δ is a small positive number, then sampling $\rho_+ \geq (1 + \delta)\rho \log(\rho)$ coordinates is sufficient in order to ensure that $\sigma_\rho(UH) \geq \delta$ with failure probability $O(\rho^{-\delta c})$ for a positive constant c . Moreover, according to [HMT11, Section 11.2], the choice of $\rho_+ = \rho + 20$ is adequate in almost all applications.

Remark C.2. In the case of using SRFT multipliers, Theorem C.1 bounds the failure probability by $O(1/\rho)$. For comparison, in the case of using Gaussian multipliers, the upper bound on the failure probability has order $1/2^{n-\rho}$ by virtue of Theorem B.3.

D Circulant, subcirculant, and Toeplitz matrices

An $n \times n$ circulant matrix $Z = (z_{i-j \bmod n})_{i,j=0}^{n-1} = \Omega^{-1}D\Omega$ is defined by its first column $\mathbf{z} = (z_i)_{i=0}^{n-1}$ or by the diagonal matrix $D = \text{diag}(d_i)_{i=0}^{n-1}$ where $(d_i)_{i=0}^{n-1} = \sqrt{n} \Omega \mathbf{z}$ and $\Omega^{-1} = \Omega^H$ is the Hermitian transpose of Ω . The following fact links circulant and SRFT matrices.

Fact D.1. $\sqrt{n/\rho_+}\Omega ZR$ is a SRFT matrix for $Z = \Omega^{-1}D\Omega$ provided that the diagonal entries d_0, \dots, d_{n-1} of the matrix D are independent and uniformly distributed on the complex unit circle $\{x : |x| = 1\}$ and R is the random $n \times \rho$ matrix defined in the beginning of the previous section.

A circulant matrix $Z = Z(\mathbf{z})$ is real if and only if its first column \mathbf{z} is real.

$k \times l$ Toeplitz matrices $T = (t_{i,j})_{i,j=0}^{m-1, n-1}$ extend the class of circulant matrices and can be defined as block submatrices of $(k+l) \times (k+l)$ circulant matrices. Such a matrix is defined by the $k+l-1$ entries of its first row and its first column.

An $n \times n$ random circulant matrix $Z = Z(\mathbf{z})$ tends to be well-conditioned [PSZ15], and hence so do its $n \times k$ and $k \times n$ Toeplitz blocks B (we call them *subcirculant*), defined by the n entries of their first row or column. Indeed, $\kappa(B) \leq \kappa(Z(\mathbf{z}))$ for such blocks B .

The known upper bounds on the condition number of a random $n \times k$ Toeplitz matrix, defined by $n+k-1$ random entries of the first row and the first column, are much greater (cf. [PSZ15]).

We only need $O(n \log(n))$ flops in order to multiply by a vector the $n \times n$ matrix Ω , and therefore $n \times n$ SRFT, circulant, subcirculant, and Toeplitz matrices as well. Similar properties hold for f -circulant matrices for a complex scalar f such that $|f| = 1$ (cf. [P01, Section 2.6]), which turn into circulant matrices for $f = 1$. Using such matrices (for a fixed or random value f), instead of circulant ones, allows further variations of our algorithms.

E Matrices Having Small Rank or Small Numerical Rank

Fact E.1. (Cf. [BV88, Proposition 1].) The set \mathbb{A} of $m \times n$ matrices of rank ρ is an algebraic variety of dimension $(m+n-\rho)\rho$ in the space $\mathbb{R}^{m \times n}$. (Clearly, $(m+n-\rho)\rho < mn$ for $\rho < \min\{m, n\}$.)

Proof. Let A be an $m \times n$ matrix of a rank ρ with a nonsingular leading $\rho \times \rho$ block B and write $A = \begin{pmatrix} B & C \\ D & E \end{pmatrix}$. Then the $(m-\rho) \times (n-\rho)$ Schur complement $E - DB^{-1}C$ must vanish, which imposes $(m-\rho)(n-\rho)$ algebraic equations on the entries of the matrix A . Similar argument can be applied in the case where any $\rho \times \rho$ submatrix of the matrix A (among $\binom{m}{\rho} \binom{n}{\rho}$ such submatrices) is nonsingular. Therefore $\dim \mathbb{A} = mn - (m-\rho)(n-\rho) = (m+n-\rho)\rho$. \square

Remark E.1. How large is the class of $m \times n$ matrices having numerical rank ρ ? We characterize it indirectly, by noting that by virtue of Fact E.1 the nearby matrices of rank ρ form a variety of dimension $(m+n-\rho)\rho$, which increases as ρ increases.

Acknowledgements: Our work has been supported by NSF Grant CCF-1116736 and PSC CUNY Awards 4512-0042 and 65792-0043. We are also grateful to a reviewer for valuable comments.

References

- [BP94] D. Bini, V. Y. Pan, *Polynomial and Matrix Computations*, Volume 1: Fundamental Algorithms, Birkhäuser, Boston. 1994.
- [BV88] W. Bruns, U. Vetter, *Determinantal Rings, Lecture Notes in Math.*, **1327**, Springer, Heidelberg, 1988.
- [CD05] Z. Chen, J. J. Dongarra, Condition Numbers of Gaussian Random Matrices, *SIAM J. on Matrix Analysis and Applications*, **27**, 603–620, 2005.

- [D88] J. Demmel, The Probability That a Numerical Analysis Problem Is Difficult, *Math. of Computation*, **50**, 449–480, 1988.
- [DS01] K. R. Davidson, S. J. Szarek, Local Operator Theory, Random Matrices, and Banach Spaces, in *Handbook on the Geometry of Banach Spaces* (W. B. Johnson and J. Lindenstrauss editors), pages 317–368, North Holland, Amsterdam, 2001.
- [E88] A. Edelman, Eigenvalues and Condition Numbers of Random Matrices, *SIAM J. on Matrix Analysis and Applications*, **9**, **4**, 543–560, 1988.
- [ES05] A. Edelman, B. D. Sutton, Tails of Condition Number Distributions, *SIAM J. on Matrix Analysis and Applications*, **27**, **2**, 547–560, 2005.
- [GL13] G. H. Golub, C. F. Van Loan, *Matrix Computations*, Johns Hopkins University Press, Baltimore, Maryland, 2013 (4th addition).
- [GOSTZ10] S. Goreinov, I. Oseledets, D. Savostyanov, E. Tyrtyshnikov, and N. Zamarashkin, How to find a good submatrix, in *Matrix Methods: Theory, Algorithms, Applications*, (dedicated to the Memory of Gene Golub, edited by V. Olshevsky and E. Tyrtyshnikov), pages 247–256, World Scientific Publishing, New Jersey, ISBN-13 978-981-283-601-4, ISBN-10-981-283-601-2 2010.
- [GT01] S. A. Goreinov and E. E. Tyrtyshnikov, The maximal-volume concept in approximation by low-rank matrices, *Contemporary Mathematics*, **208**, 47–51, 2001.
- [H02] N. J. Higham, *Accuracy and Stability in Numerical Analysis*, SIAM, Philadelphia, 2002 (second edition).
- [HMT11] N. Halko, P. G. Martinsson, J. A. Tropp, Finding Structure with Randomness: Probabilistic Algorithms for Constructing Approximate Matrix Decompositions, *SIAM Review*, **53**, **2**, 217–288, 2011.
- [P01] V. Y. Pan, *Structured Matrices and Polynomials: Unified Superfast Algorithms*, Birkhäuser/Springer, Boston/New York, 2001.
- [P10] V. Y. Pan, Newton’s Iteration for Matrix Inversion, Advances and Extensions, pp. 364–381, in *Matrix Methods: Theory, Algorithms and Applications* (dedicated to the Memory of Gene Golub, edited by V. Olshevsky and E. Tyrtyshnikov), pages 364–381, World Scientific Publishing, New Jersey, ISBN-13 978-981-283-601-4, ISBN-10-981-283-601-2 (2010).
- [P15] V. Y. Pan, Transformations of matrix structures work again, *Linear Algebra and Its Applications*, **465**, 1–32, 2015.
- [PGMQ08] V. Y. Pan, D. Grady, B. Murphy, G. Qian, R. E. Rosholt, A. Ruslanov, Schur Aggregation for Linear Systems and Determinants, *Theoretical Computer Science, Special Issue on Symbolic–Numerical Algorithms* (D. A. Bini, V. Y. Pan, and J. Verschelde editors), **409**, **2**, 255–268, 2008.
- [PIMR08a] V. Y. Pan, D. Ivolgin, B. Murphy, R. E. Rosholt, I. Taj-Eddin, Y. Tang, X. Yan, Additive Preconditioning and Aggregation in Matrix Computations, *Computers and Mathematics with Applications*, **55**, **8**, 1870–1886, 2008.
- [PIMR08b] V. Y. Pan, D. Ivolgin, B. Murphy, R. E. Rosholt, Y. Tang, X. Yan, Additive Preconditioning for Matrix Computations, in *Proc. of the Third International Computer Science Symposium in Russia (CSR’2008)*, *Lecture Notes in Computer Science (LNCS)*, **5010**, 372–383, 2008.

- [PIMR10] V. Y. Pan, D. Ivolgin, B. Murphy, R. E. Rosholt, Y. Tang, X. Yan, Additive Preconditioning for Matrix Computations, *Linear Algebra and Its Applications*, **432**, 1070–1089, 2010.
- [PKRK06] V. Y. Pan, M. Kunin, R. Rosholt, H. Kodai, Homotopic Residual Correction Algorithms for General and Structures Matrices, *Math. of Computation*, **75**, 345–368, 2006.
- [PMRT07] V. Y. Pan, B. Murphy, R. E. Rosholt, M. Tabanjeh, Null Space and Eigenspace Computation with Additive Preconditioning, *Proceedings of the Third International Workshop on Symbolic–Numeric Computation (SNC’2007)*, July 2007, London, Ontario, Canada (Jan Verschelde and Stephen Watt, editors), 170–179, ACM Press, New York, 2007.
- [PQ10] V. Y. Pan, G. Qian, Randomized Preprocessing of Homogeneous Linear Systems of Equations, *Linear Algebra and Its Applications*, **432**, 3272–3318, 2010.
- [PQ12] V. Y. Pan, G. Qian, Solving Linear Systems of Equations with Randomization, Augmentation and Aggregation, *Linear Algebra and Its Applications*, **437**, 2851–1876, 2012.
- [PQY15] V. Y. Pan, G. Qian, X. Yan, Random Multipliers Numerically Stabilize Gaussian and Block Gaussian Elimination: Proofs and an Extension to Low-rank Approximation, *Linear Algebra and Its Applications*, **481**, 202–234, 2015.
- [PQZ13] V. Y. Pan, G. Qian, A. Zheng, Randomized Preprocessing versus Pivoting, *Linear Algebra and Its Applications*, **438**, 4, 1883–1899, 2013.
- [PQZC] V. Y. Pan, G. Qian, A. Zheng, Z. Chen, Matrix Computations and Polynomial Root-finding with Preprocessing, *Linear Algebra and Its Applications*, **434**, 854–879, 2011.
- [PSZ15] V. Y. Pan, J. Svadlenka, L. Zhao, Estimating the Norms of Circulant and Toeplitz Random Matrices and Their Inverses, *Linear Algebra and Its Applications*, **468**, 197–210, 2015.
- [PY07] Null Space and Eigenspace Computation with Additive Preconditioning, *Proceedings of the Third International Workshop on Symbolic–Numeric Computation (SNC’2007)*, July 2007, London, Ontario, Canada (Jan Verschelde and Stephen Watt, editors), 170–179, ACM Press, New York, 2007.
- [PY09] V. Y. Pan, X. Yan, Additive Preconditioning, Eigenspaces, and the Inverse Iteration, *Linear Algebra and Its Applications*, **430**, 186–203, 2009.
- [PZ15] V. Y. Pan, L. Zhao, Randomized Circulant and Gaussian Preprocessing, Proceedings of the 17th International Workshop on Computer Algebra in Scientific Computing (CASC’2015), (V. P. Gerdt, V. Koepf, and E. V. Vorozhtsov, editors), Lecture Notes in Computer Science, Springer, Heidelberg (2015), accepted.
- [PZa] V. Y. Pan, L. Zhao, How Much Randomness Do We Need for Supporting Gaussian Elimination, Block Gaussian Elimination, and Low-rank Approximation? arxiv 1501.05385 CS (36 pages, 12 figures), submitted on January 22, 2015, revised on October 21, 2015.
- [PZb] Low-rank Approximation of a Matrix: Novel Insights, New Progress, and Extensions” by V. Y. Pan, L. Zhao, arXiv:1510.06142 [math.NA] (16 pages, 3 tables), submitted on 21 Oct 2015, revised on 14 March 2016.
- [S95] J.-G. Sun, On Perturbation Bounds for QR Factorization, *Linear Algebra and Its Applications*, **215**, 95–111, 1995.

- [S98] G. W. Stewart, *Matrix Algorithms, Vol I: Basic Decompositions*, SIAM, Philadelphia, 1998.
- [SST06] A. Sankar, D. Spielman, S.-H. Teng, Smoothed Analysis of the Condition Numbers and Growth Factors of Matrices, *SIAM J. on Matrix Analysis*, **28**, **2**, 446–476, 2006.
- [W07] X. Wang, Affect of Small Rank Modification on the Condition Number of a Matrix, *Computer and Math. (with Applications)*, **54**, 819–825, 2007.